

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT)
FOR E-MAIL ACCOUNT)
Redacted)
MAINTAINED ON COMPUTER SERVERS)
OPERATED BY GOOGLE, INC.,)
HEADQUARTERED AT)
1600 AMPHITHEATRE PARKWAY,)
MOUNTAIN VIEW, CA)

Misc. No.: 10-291-M-01

UNDER SEAL

ORDER

After reviewing the United States' May 21, 2013, Motion to Unseal Entire Docket, it is hereby

ORDERED that the United States' motion is **GRANTED**; it is

FURTHER ORDERED that the Clerk of the Court **UNSEAL** and place on the public docket redacted versions of the documents attached as Exhibits A through S to the United States' Motion to Unseal; it is

FURTHER ORDERED that the Clerk of the Court shall place on the public docket a redacted version of the Motion to Unseal Entire Docket and this Order, removing from the caption the name of the email account at issue (proposed versions of which were attached to the United States' Motion to Unseal Entire Docket as Exhibit T and U); and

FURTHER ORDERED that the United States may produce unredacted versions of all of the unsealed material to the defense in United States v. Stephen Jin-Woo Kim, Cr. No. 10-225 (CKK), pursuant to the Rule 16 Protective Order in that matter.

SO ORDERED this 22nd day of May 2013.


United States District Court

EXHIBIT A

**UNITED STATES MAGISTRATE JUDGE
U.S. DISTRICT COURT BUILDING
WASHINGTON, D.C.**

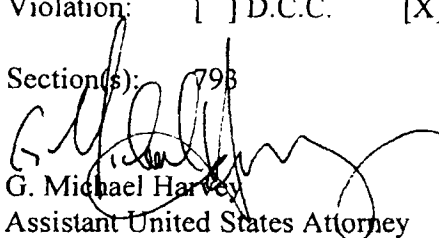
70-291-M-01

PLEASE ISSUE: ☐ Arrest ☒ Search ☒ Seizure

warrant for: E-mail Account [REDACTED]@gmail.com Maintained on
Computer Servers Operated by Google, Inc., Headquartered at 1600
Amphitheatre Parkway, Mountain View, California

Violation: ☐ D.C.C. ☒ U.S.C. Title: 18

Section(s): 798


G. Michael Harley
Assistant United States Attorney
(202) 305-4155

May 28, 2010

Date

Bond: _____

COMPLETE FOR ALL ARREST WARRANTS:

*The following information must be provided for ALL arrest warrants and an **original** and **duplicate** of this form must be submitted to the Clerk's Office with the warrant papers.*

Officer / Agent Name: Special Agent Reginald B. Reyes

Badge Number:

Agency / Unit: Federal Bureau of Investigation

24 Hour Telephone Number: (202) 278-4868
(For officer/agent)

Cell Number:
(For officer/agent) 202-345-9382

EXHIBIT B

THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT)
FOR E-MAIL ACCOUNT)
[REDACTED]@GMAIL.COM)
MAINTAINED ON COMPUTER SERVERS)
OPERATED BY GOOGLE, INC.,)
HEADQUARTERED AT)
1600 AMPHITHEATRE PARKWAY,)
MOUNTAIN VIEW, CA)

Misc. No.:

10-291-M-01

UNDER SEAL

FILED

MAY 28 2010

MOTION TO SEAL SEARCH WARRANT AND RELATED MATERIALS AND FOR
NON-DISCLOSURE

Clerk, U.S. District & Bankruptcy
Court for the District of Columbia

The United States, by and through its attorney, the United States Attorney for the District of Columbia respectfully requests that the Court issue an Order to Seal the search warrant and related materials, including the application for the search warrant, the affidavit in support of the search warrant, the memorandum in support thereof, and the subsequent return on the search warrant, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal the materials.

The Court has the inherent power to seal search warrants and their related materials to protect an ongoing investigation. United States v. Hubbard, 650 F.2d 293 (D.C. Cir. 1980). Moreover, under Post v. Robinson, 935 F.2d 282, 289 n.10 (D.C. Cir. 1991), the court may seal filings where there exists an extraordinary situation and a compelling governmental interest which justify such sealing.

FACTS

In June 2009, TOP SECRET United States national defense information was published in an article on a national news organization's website (hereinafter the "June 2009 article"). Following that unauthorized disclosure, an FBI investigation was initiated to determine the source(s) of the disclosure. The investigation has revealed that one individual who both accessed the classified information at issue, and communicated with the reporter who wrote the June 2009 article, was

UNDER SEAL

Stephen Jin-Woo Kim. One way that Mr. Kim communicated with the reporter was by email to one of the reporter's email accounts, [REDACTED]@gmail.com – the account that is the subject of the present search warrant. The FBI is currently engaged in an ongoing investigation of the leak that will be substantially and adversely affected if Mr. Kim or the reporter were to prematurely become aware of the specific details known to the FBI as a result of its investigation and/or the legal process (and targets of that legal process) that is being used during the investigation. The government submits that this constitutes a legitimate governmental interest to be protected by the requested sealing.

Moreover, ongoing investigative steps that will be taken in the wake of execution of this search warrant, such as interviews and the pursuit of other warrants and legal process, would be adversely affected if the details set forth in the Affidavit were to become publicly available at this time. This, too, constitutes a legitimate governmental interest to be protected by the requested sealing.

The United States has considered alternatives less drastic than sealing and has found none that would suffice to protect the government's legitimate interest in attempting to locate and prosecute those responsible for the bombings.

The government submits that under Post v. Robinson, 935 F.2d 282, 289 n.10 (D.C. Cir. 1991), these facts present an extraordinary situation and a compelling governmental interest which justify the sealing of the search warrant, the application, the affidavit, the memorandum in support thereof, and the return of the warrant as well as the instant Motion to Seal, and the Order to Seal, until such time as the Court orders otherwise.

UNDER SEAL

CONCLUSION

WHEREFORE, the United States respectfully requests that the search warrant, the application for the search warrant, the affidavit in support of the search warrant, the memorandum in support thereof, the return of the search warrant and this Motion to Seal and proposed Order be sealed until the United States moves to unseal. A proposed Order is submitted herewith.

Respectfully submitted,

RONALD C. MACHEN JR.
UNITED STATES ATTORNEY

By: 

G. MICHAEL HARVEY
Assistant United States Attorney
D.C. Bar Number 447-465
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-439
Washington, D.C. 20530
Phone: (202) 305-4155
michael.harvey2@usdoj.gov

EXHIBIT C

IN THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT)
FOR E-MAIL ACCOUNT)
[REDACTED]@GMAIL.COM)
MAINTAINED ON COMPUTER SERVERS)
OPERATED BY GOOGLE, INC.,)
HEADQUARTERED AT)
1600 AMPHITHEATRE PARKWAY,)
SUNNYVALE, CA)

Mag.

Case No.:

10-291-M-01

UNDER SEAL

FILED

MAY 28 2010

ORDER TO SEAL

Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

Having considered the Government's Motion for an Order to Seal Search Warrant and Related Materials and for Non-disclosure ("Government's Motion"), in connection with the above-captioned matter, and having found that sealing the search warrant and all attachments thereto, the application for the search warrant, the affidavit in support of the search warrant, the memorandum in support thereof, the subsequent return of the search warrant, and the government's motion and proposed order will further the legitimate prosecutorial interest in preserving the integrity of an ongoing criminal investigation, and having therefore concluded that there is a compelling governmental interest in sealing said documents, and having further concluded that notification of the government's access to the e-mail account in question would seriously jeopardize an ongoing criminal investigation,

the Government's Motion is **HEREBY GRANTED**; it is further

ORDERED that the Search Warrant and attachments thereto, the Application for the Search Warrant, Affidavit in Support of the Search Warrant in this matter, the Memorandum in Support Thereof, the subsequent Return of the Search Warrant, the Government's Motion and this Order be sealed until further order of this Court; it is further

ORDERED that, pursuant to Title 18, United States Code, Section 2705(b), Google, Inc.,

and its employees and agents are prohibited from notifying the subscriber(s) of the above-listed e-mail address, or any other unauthorized person, in any manner, of the existence of the search warrant or application and any work or request for work conducted in response to the search warrant; and it is further

ORDERED that the Clerk's Office shall provide to the U.S. Attorney's Office three (3) certified copies of the Search Warrant and related pleadings in this case.

Nothing in this Order shall prohibit the government from providing this Order or the Search Warrant and its attachment, to Google, Inc., or Google, Inc., from providing the same to its authorized employees, so that the warrant can be executed.



U.S. DISTRICT COURT MAGISTRATE JUDGE
ALAN KAY
U.S. MAGISTRATE JUDGE

Serve: G. Michael Harvey
Assistant United States Attorney
National Security Section
555 4th Street, N.W., Room 11-439
Washington, D.C. 20530
(202) 305-4155
michael.harvey2@usdoj.gov

EXHIBIT D

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of ColumbiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)E-mail Account [REDACTED]@gmail.com on
Computer Servers Operated by Google, Inc., 1600
Amphitheatre Parkway, Mountain View, California

Case No. 10-291-M-01

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Northern District of California

(identify the person or describe the property to be searched and give its location):

E-mail account [REDACTED]@gmail.com, maintained on computer servers operated by Google, Inc., headquartered
at 1600 Amphitheatre Parkway, Mountain View, California.The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):Certain property, the disclosure of which is governed by Title 42, U.S.C. Section 2000aa, and Title 18, U.S.C. Sections
2701 through 2711, namely contents of electronic e-mails and other electronic data, more fully described in
ATTACHMENT A to this application.I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before

JUN 11 2010

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

(name)

☒ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☒ for 30 days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____.

MAY 28 2010

Date and time issued: _____

City and state: District of Columbia

Judge's Signature

ALAN KAY
U.S. MAGISTRATE JUDGE
Printed name and title

Printed name and title

EXHIBIT E

THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT)
FOR E-MAIL ACCOUNT)
[REDACTED]@GMAIL.COM)
MAINTAINED ON COMPUTER SERVERS)
OPERATED BY GOOGLE, INC.,)
HEADQUARTERED AT)
1600 AMPHITHEATRE PARKWAY,)
MOUNTAIN VIEW, CA)

Mag 10-mj-291
Misc. No.: 10-291-M-01(AK)

UNDER SEAL

FILED

JUN - 8 2010

Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

MOTION FOR CLARIFICATION OF NOTICE OBLIGATIONS OF
E-MAIL SEARCH WARRANT

On May 28, 2010, the United States, by and through its attorney, the United States Attorney for the District of Columbia, sought a search warrant from this Court for the e-mail account [REDACTED]@gmail.com. See Application for Search Warrant attached as Exhibit 1 hereto. That same day, this Court granted that request. See Search and Seizure Warrant attached as Exhibit 2 hereto. When signing the warrant, this Court checked the box on the face of the warrant finding that immediate notification of the warrant "to the person who, or whose property, will be searched or seized" would "have an adverse result listed in 18 U.S.C. §2705" and permitted delayed notification for up to 30 days. See id. The United States did not seek such delayed notification in this case, however, because, it respectfully submits, there is no such notice obligation for e-mail search warrants under 18 U.S.C. § 2703(b)(1)(A). Accordingly, this motion seeks clarification that the United States has no notice obligation to the customer or subscriber of the [REDACTED]@gmail.com account (whether in 30 days or thereafter).

The language of section 2703(b)(1) states that:

- (1) A government entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication . . .
 - (A) *without required notice to the subscriber or customer, if the government entity obtains a warrant issued using the procedures described in the*

A

UNDER SEAL

Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction; or

(B) *with prior notice* from the governmental entity to the subscriber or customer if the government entity —

(I) uses an administrative *subpoena* authorized by a Federal or State statute or a Federal or State Grand jury or trial subpoena; or
(ii) obtains a *court order* for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

18 U.S.C. §2703(b)(1) (emphasis added). Thus, with regard to e-mail accounts, the delayed notice provisions under section 2705 are applicable only if the Government were seeking the content of e-mails either through a subpoena or a court order under 18 U.S.C. §2703(d). See id.; see also 18 U.S.C. § 2705(a) (providing for delayed notice to subscribers and customers for “court orders” and “subpoenas”). Where, as here, the Government seeks such contents through a search warrant, no notice to the subscriber or customer of the e-mail account is statutorily required or necessary.¹ Thus, this Court’s indication on the face of the warrant that delayed notice of 30 days to the customer and subscriber was permissible in this case was unnecessary

¹ The Government’s affidavit in support of the search warrant application requested that the Court order the e-mail service provider, Google, Inc., not to notify the customer or subscriber of the warrant seeking the contents of the e-mail accounts. Such relief was made a part of the Attachment A to the warrant that this Court issued as part of the warrant. See Attachment A attached as Exhibit 3 hereto. Such relief is permitted under 18 U.S.C. § 2705(b), and exists separate and apart from any (non-existent) Government obligation to provide notice to the subscriber or customer of e-mail accounts searched and seized under section 2703(b)(1)(A).

UNDER SEAL

and could result in confusion and litigation about the Government's notice obligations regarding the warrant in future. To the extent the Court was directing the Government to provide such notice to the subscriber or customer of the [REDACTED]@gmail.com account within 30 days, such a requirement is contrary to the language of the statute.

The Government believes that the new search and seizure warrant form issued by the Administrative Office of the United States Courts (AO) is responsible for the confusion the Government seeks to clarify here. The prior search warrant form used by this Court had no such delayed notification provision on the face of the form. The Government believes that the new form's reference to delayed notification under section 2705 refers only to the delayed notice permitted in the Patriot Act for covert (or "sneak and peak") searches and seizures of property under 18 U.S.C. §3103a, not, as here, a warrant for a search of an e-mail account under section 2703(b)(1)(A). See 18 U.S.C. § 3103a(b)(1)(making reference to the section 2705's "adverse result" standard in permitting delayed notice for covert searches of property under Rule 41). The Government has for years sought e-mail search warrants using the old form and, consistent with the language of section 2703(b)(1)(A), has not sought delayed notification from the Court for those warrants. Nor is it its regular practice to provide pre-indictment notice of those warrants to the subscribers and customers of the e-mail accounts so searched and seized. The new form, however, makes no distinction between covert physical searches and searches of e-mail accounts under section 2703(b)(1)(A). Because the new form will be used both for warrants for searches of physical property where notice is statutorily required and for searches of the contents of e-mail accounts where it is not, the confusion caused by the language of the form is likely to continue. The undersigned is seeking to bring this issue to the attention of the AO.

UNDER SEAL

Accordingly, the Government respectfully requests that the Court clarify that the Government has no notice obligation to the subscriber and customer of the target e-mail account concerning the warrant at issue. Further, the United States respectfully requests that, like the rest of the docket in this matter, this motion and the proposed Order be sealed until further order of the Court. A proposed Order is submitted herewith.

Respectfully submitted,

RONALD C. MACHEN JR.
UNITED STATES ATTORNEY

By:

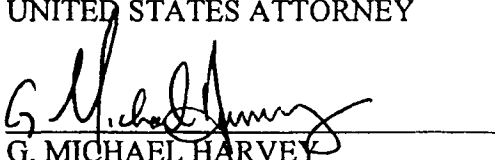

G. MICHAEL HARVEY
Assistant United States Attorney
D.C. Bar Number 447-465
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-439
Washington, D.C. 20530
Phone: (202) 305-4155
michael.harvey2@usdoj.gov

EXHIBIT 1

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)E-mail Account [REDACTED]@gmail.com on
Computer Servers Operated by Google, Inc., 1600
Amphitheatre Parkway, Mountain View, California

Case No.

70-291-M-01

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
e-mail account [REDACTED]@gmail.com, maintained on computer servers operated by Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, California,

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

certain property, the disclosure of which is governed by Title 42, U.S.C. Section 2000aa, and Title 18, U.S.C. Sections 2701 through 2711, namely contents of electronic e-mails and other electronic data and more fully described in ATTACHMENT A to this application.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

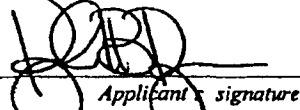
- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 793	Gathering, transmitting or losing defense information

The application is based on these facts:
See attached affidavit herein incorporated by reference as if fully restated herein.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Reginald B. Reyes, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: MAY 28 2010

City and state: Washington, D.C.



Judge's signature

ALAN KAY

U.S. MAGISTRATE JUDGE

EXHIBIT 2

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of ColumbiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)E-mail Account [REDACTED]@gmail.com on
Computer Servers Operated by Google, Inc., 1600
Amphitheatre Parkway, Mountain View, California

Case No. 10-291-M-01

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Northern District of California

(identify the person or describe the property to be searched and give its location):

E-mail account [REDACTED]@gmail.com, maintained on computer servers operated by Google, Inc., headquartered
at 1600 Amphitheatre Parkway, Mountain View, California.The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):Certain property, the disclosure of which is governed by Title 42, U.S.C. Section 2000aa, and Title 18, U.S.C. Sections
2701 through 2711, namely contents of electronic e-mails and other electronic data, more fully described in
ATTACHMENT A to this application.I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before

JUN 11 2010

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

(name)

☒ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for 30 days (not to exceed 30).☐ until, the facts justifying, the later specific date of

Date and time issued:

MAY 28 2010

District of Columbia

City and state:

Judge's signature
ALAN KAY
U.S. MAGISTRATE JUDGE
Printed name and title

EXHIBIT 3

ATTACHMENT A: ITEMS TO BE SEIZED

Pursuant to 18 U.S.C. § 2703 and 42 U.S.C. § 2000aa(a), it is hereby ordered as follows:

I. SERVICE OF WARRANT AND SEARCH PROCEDURE

a. Google, Incorporated, a provider of electronic communication and remote computing services, located at 1600 Amphitheatre Parkway, Mountain View, California, (the "PROVIDER") will isolate those accounts and files described in Section II below. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

b. The PROVIDER shall not notify any other person, including the subscriber(s) of [REDACTED]@gmail.com of the existence of the warrant.

c. In order to minimize any disruption of computer service to innocent third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

d. As soon as practicable after service of this warrant, the PROVIDER shall provide the exact duplicate in electronic form of the account and files described in Section II below and all information stored in that account and files to the following FBI special agent:

Reginald B. Reyes
FBI-WFO
601 4th Street, NW
Washington, D.C. 20535
Fax: 202-278-2864
Desk: 202-278-4868

The PROVIDER shall send the information to the agent via facsimile and overnight mail, and where maintained in electronic form, on CD-ROM or an equivalent electronic medium.

e. The FBI will make an exact duplicate of the original production from the PROVIDER. The original production from the PROVIDER will be sealed by the FBI and preserved for authenticity and chain of custody purposes.

II. FILES AND ACCOUNTS TO BE COPIED BY THE PROVIDER'S EMPLOYEES

a. Any and all communications, on whatever date, between

██████████@gmail.com ("SUBJECT ACCOUNT") and any of the following accounts:

- (1) ██████████@yahoo.com,
- (2) ██████████@yahoo.com, and
- (3) ██████████@gmail.com.

"Any and all communications" includes, without limitation, received messages (whether "to," "cc'd," or "bcc'd" to the SUBJECT ACCOUNT), forwarded messages, sent messages (whether "to," "cc'd," or "bcc'd" to the three above-listed accounts), deleted messages, and messages maintained in trash or other folders, and any attachments thereto, including videos, documents, photos, internet addresses, and computer files sent to and received from other websites. "Any and all communications" further includes all prior email messages in an email "chain" between the SUBJECT ACCOUNT and any of the three above-listed accounts, whether or not those prior emails were in fact sent between the SUBJECT ACCOUNT and the above-listed accounts;

b. Any and all communications "to" or "from" the SUBJECT ACCOUNT on June 10 and/or June 11, 2009. "Any and all communications" includes, without limitation, received messages (whether "to," "cc'd," or "bcc'd" to the SUBJECT ACCOUNT), forwarded messages, sent messages, deleted messages, messages maintained in trash or other folders, and any

attachments thereto, including videos, documents, photos, internet addresses, and computer files

sent to and received from other websites. "Any and all communications" further includes all prior email messages in an email "chain" sent "to" or "from" the SUBJECT ACCOUNT on June 10 or June 11, 2009, whether or not those prior emails in the "chain" were in fact sent or received on June 10 or June 11, 2009;

c. All existing printouts from original storage of all of the electronic mail described above in Section II (a) and II(b);

d. All transactional information of all activity of the SUBJECT ACCOUNT described above in Section II(a) and II(b), including log files, dates, times, methods of connecting, ports, dial-ups, registration Internet Protocol (IP) address and/or locations;

e. All business records and subscriber information, in any form kept, pertaining to the SUBJECT ACCOUNT described above in Section II(a) and II(b), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, account numbers, screen names, status of accounts, dates of service, methods of payment, telephone numbers, addresses, detailed billing records, and histories and profiles;

f. All records indicating the account preferences and services available to subscribers of the SUBJECT ACCOUNT described above in Section II(a) and II(b).

III. INFORMATION TO BE SEIZED BY LAW ENFORCEMENT PERSONNEL

Items to be seized, which are believed to be evidence and fruits of violations of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information) as follows:

a. The contents of electronic communications, including attachments and stored
files, for the SUBJECT ACCOUNT as described and limited by Section II(a) and II(b) above,

including videos, computer files sent to and received from other websites, received messages, sent messages, deleted messages, messages maintained in trash or other folders, any attachments thereto, and all existing printouts from original storage of all of the electronic mail described above in Section II(a) and II(b), that pertain to:

1. records or information related to violations of 18 U.S.C. § 793;
 2. any and all communications between Stephen Kim and the author of the article (the “Author”) that is the subject matter of the FBI investigation that is the basis for this warrant (the “Article”) and any record or information that reflects such communications;
 3. records or information relating to Stephen Kim’s communications and/or activities on the date of publication of the Article;
 4. records or information relating to the Author’s communication with any other source or potential source of the information disclosed in the Article;
 5. records or information related to Stephen Kim’s or the Author’s knowledge of laws, regulations, rules and/or procedures prohibiting the unauthorized disclosure of national defense or classified information;
 6. records or information related to Stephen Kim’s or the Author’s knowledge of government rules and/or procedures regarding communications with members of the media;
 7. records or information related to any disclosure or prospective disclosure of classified and/or intelligence information;
-
8. any classified document, image, record or information, and any

communications concerning such documents, images, records, or information;

9. any document, image, record or information concerning the national defense, including but not limited to documents, maps, plans, diagrams, guides, manuals, and other Department of Defense, U.S. military, and/or weapons material, as well as sources and methods of intelligence gathering, and any communications concerning such documents, images, records, or information;
10. records or information related to the state of mind of any individuals seeking the disclosure or receipt of classified, intelligence and/or national defense information;
11. records or information related to the subject matter of the Article; and
12. records or information related to the user(s) of the SUBJECT ACCOUNT.

b. All of the records and information described above in Sections II(d), II(e), and II(f) including:

1. Account information for the SUBJECT ACCOUNT including:
 - (a) Names and associated email addresses;
 - (b) Physical address and location information;
 - (c) Records of session times and durations;
 - (d) Length of service (including start date) and types of service utilized;
 - (e) Telephone or instrument number or other subscriber number or identity,

including any temporarily assigned network address;

(f) The means and source of payment for such service (including any credit card or bank account number); and

(g) Internet Protocol addresses used by the subscriber to register the account or otherwise initiate service.

2. User connection logs for the SUBJECT ACCOUNT for any connections to or from the SUBJECT ACCOUNT. User connection logs should include the following:

- (a) Connection time and date;
- (b) Disconnect time and date;
- (c) Method of connection to system (e.g., SLIP, PPP, Shell);
- (d) Data transfer volume (e.g., bytes);
- (e) The IP address that was used when the user connected to the service,
- (f) Connection information for other systems to which user connected via the SUBJECT ACCOUNT, including:

- (1) Connection destination;
 - (2) Connection time and date;
 - (3) Disconnect time and date;
 - (4) Method of connection to system (e.g., telnet, ftp, http);
 - (5) Data transfer volume (e.g., bytes);
 - (6) Any other relevant routing information.
-

EXHIBIT F

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT
FOR E-MAIL ACCOUNT
[REDACTED]@GMAIL.COM
MAINTAINED BY GOOGLE, INC.,
HEADQUARTERED AT 1600
AMPHITHEATRE PARKWAY,
SUNNYVALE, CA

Mag. No. 10-mj-291 (AK/JMF)
(Under seal)

MEMORANDUM ORDER

The government has filed a Motion for Clarification of Notice Obligations of E-mail Search Warrant ("Mot."), seeking clarification of the Court's decision to check the box on the face of the warrant finding that immediate notification of the warrant "to the person who, or whose property, will be searched or seized" would "have an adverse result listed in 18 U.S.C. § 2705" and permitting delayed notification for up to 30 days. See Mot. at Ex. 2, Search and Seizure Warrant ("Warrant").

I. Introduction

In an opinion I wrote several years ago, I questioned whether a person's location as detected by the use of geolocation information created by her cell phone could ever constitute evidence subject to seizure under Rule 41 of the Federal Rules of Criminal Procedure.¹ Then-Chief Judge Hogan reviewed the denial of an application for such a

¹ In that opinion, I indicated that "if the government's quoted statement is an invocation of the Fourth Amendment standard, it fails to capture the entire force of that Amendment—that it permits the issuance of a warrant upon a showing that there is probable cause to believe that whatever is to be seized is '(1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime.' Fed. R. Crim. P. 41(c); Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 308 (1967). Putting aside the complicated question of whether a person's location could in itself meet any of these criteria, it is

warrant by another magistrate judge in the Court and determined that a person's location could be evidence of a crime. See In re U.S. for an Order Authorizing Monitoring of Geolocation and Cell Site Data for a Sprint Spectrum Cell Phone Number, Nos. 06-mc-186, 187, and 188, 2006 WL 6217584, at *4 n.6 (D.D.C. Aug. 25, 2006) (finding that "[c]ell site and geolocation information may be evidence of a crime because, for example, a subject's location can be used to rebut an alibi or place him at the scene of a crime"). Ever since that decision, the United States Attorney's Office for the District of Columbia (USAO), while protecting its objection that it is not required to show probable cause in each application, has consistently made a showing of probable cause when seeking prospective geolocation data.

In seeking geolocation data, the government typically also invokes 18 U.S.C. § 3103a(b),² which allows any required notice of the warrant to be delayed in certain circumstances. See 18 U.S.C. § 3103a(b). When granting such a delay under this statute, the Court is required to report the approval of such a delay to the Administrative Office of the United States Courts ("AO"). See 18 U.S.C. § 3103a(d). The AO revised its search warrant form, recommended for use by the federal courts, to include a box that the issuing judge must check to indicate that she has found reasonable cause to approve a delay in notifying the party subject to the search of the existence of a warrant. See AO

certainly clear that probable cause to believe that a person's location is relevant to a criminal investigation cannot possibly meet the constitutional standard the government purports to invoke, that it is more likely than not that what is [to] be seized is evidence, contraband, fruits of a crime or designed to be used to commit a crime." In re Application of U.S. for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 132, 133 (D.D.C. 2005).

² All references to the United States Code are to the electronic version in Westlaw or Lexis.

93 (Rev. 12/09) Search and Seizure Warrant. The judge then specifies on the warrant the number of days such notice may be delayed. Id. This is done pursuant to the statutory authority granted by 18 U.S.C. § 3130a(b) that permits such delay in notification; but for that statute, the executing officer would have to give the party subject to the search a copy of the warrant and a receipt for what the officer has taken. Fed. R. Crim. P. 41(f)(1)(C). Thus, the government, using this form, may seek to delay notification by having the judge check the box, but it may not completely abdicate its responsibility under Rule 41(f)(1)(C); eventually, the cell phone subscriber whose whereabouts are being tracked will ultimately receive a copy of the warrant, which authorized the government to gather the geolocation data from the phone without her knowledge.

In this case, the government is not seeking geolocation data from a cell phone. Instead, the government seeks to search the contents of a person's e-mail account, pursuant to the Stored Communications Act ("SCA"). See Warrant. I only recount the history of geolocation warrants because it highlights an incongruity in the government's position. In this case, the government objects to having to provide any notice to the subscriber of the account being searched. Mot. at 1. According to the government, notice to the e-mail account provider is sufficient. The subscriber therefore will never know, by being provided a copy of the warrant, for example, that the government secured a warrant and searched the contents of her e-mail account. In comparison, the user of a cell phone whose telecommunications data has been intercepted and captured pursuant to a warrant would ultimately learn that the government has been surveilling her, even though a portion of that surveillance may have occurred when she was in a public place. The e-mail account holder, on the other hand, would never learn of the search of the entire

contents of her e-mail account. Thus, as the government would have it, while it would have to tell a person that it followed his movements one day as he walked from K Street to Connecticut Avenue, it would never have to tell him that it has read and copied the entire contents of the e-mail account that he opened when he arrived at his office on K Street.

The incongruity of that position compels to me conclude that the more appropriate interpretation of the pertinent portions of the SCA and of Rule 41 of the Federal Rules of Criminal Procedure is that Congress intended that the person whose e-mail account is seized by the government ultimately receives notice of that seizure, even though that notification may be delayed, if the requirements of the applicable statutes are met.

II. Background

On May 28, 2010, USAO sought a search warrant for a particular Google E-mail (“Gmail”) account. Mot. at 1. The Court, per Magistrate Judge Kay, granted the request, and, when signing the warrant, checked the box on the AO 93 (Rev. 12/09) Search and Seizure Warrant, which indicated that the Court found that “immediate notification of the warrant ‘to the person who, or whose property, will be searched or seized’ would ‘have an adverse result listed in 18 U.S.C. § 2705’ and permitted delayed notification for up to 30 days.” Mot. at 1 (citing AO 93 (Rev. 12/09) Search and Seizure Warrant). In its application for the search warrant, the government, however, did *not* seek delayed notification. See Mot. at Ex. 1, Application for Search Warrant. Yet, my colleague, Magistrate Judge Kay, checked the box granting delayed notification. The government now seeks to be excused from its obligations to provide notice, because it does not

believe there to be any such notice obligation for e-mail search warrants under 18 U.S.C. § 2703(b)(1)(A). Mot. at 1.

The government is incorrect in its assumption; notice of a search warrant is required, even if the warrant was issued under 18 U.S.C. § 2703(b)(1)(A). Any other interpretation of the statute would lead to the insupportable conclusion that Congress intended the government to copy and read the entirety of the e-mail messages, and yet to never be required to provide notice to the owner of the e-mail account.

III. Analysis

The SCA has proven to be enormously difficult to understand and apply, probably because the technology has advanced so rapidly since its enactment in 1986. See 18 U.S.C. § 2701 *et seq.*. The SCA protects e-mail subscribers from unlawful access or involuntary disclosure of their stored communications or records,³ but also provides for the compelled disclosure of customer communications or records. 18 U.S.C. § 2703. Under § 2703, the government can require a provider to disclose the contents of wire or electronic communications. Id. There is an anachronistic curiosity within the SCA; the governmental entity seeking the disclosure must follow different procedures based on whether the communication sought is a wire or electronic communication in “electronic storage”⁴ or in a “remote computing service.”⁵

³ 18 U.S.C. §§ 2701-02.

⁴ The definition of electronic storage is: “(1) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (2) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17)(A)-(B).

⁵ “Remote computing service” refers to “the provision to the public of computer storage or processing services by means of an electronic communications system.” 18 U.S.C. § 2711(2).

While the SCA provides definitions of these terms, they were developed before the advent of prolific and free cloud computing, where a user can sign up for a free e-mail account with a subscriber and have essentially unlimited storage for e-mails. The amount of information stored in modern American business or personal e-mail accounts can be staggering. E-mail providers compete against each other by offering storage space for free. Apple's e-mail accounts, for example, come with 20 gigabytes of free storage.⁶ Microsoft offers 10 free gigabytes of storage to student users of Outlook.⁷ Google continually adds available storage space, even as one is logging into one of its accounts.⁸ With such storage capacity, the user can be expected to store thousands of sent and received messages, even those the user has designated to be "trash."

The contents of these stored e-mails are as varied as the users, but it is surely reasonable to expect that e-mail accounts contain banking, tax, and other financial information as well as more personal and intimate communications.

With its warrant, the government seeks the contents of a Gmail account under §2703(b)(1)(A), which refers to contents in a remote computing service and reads:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection -

⁶ See Apple MobileMe Home Page, <http://www.apple.com/mobileme/pricing/> (last visited Jul. 20, 2010).

⁷ See Microsoft Live@Edu Home Page, <http://www.microsoft.com/liveedu/free-hosted-student-email.aspx> (last visited Jul. 20, 2010)

⁸ See Gmail by Google Home Page, <http://mail.google.com/mail> (last visited Jul. 20, 2010).

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity –

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

18 U.S.C. § 2703(b).

The government may therefore, without notice to the subscriber, apply for a search warrant, invoking the powers and limitations of Rule 41 of the Federal Rules of Criminal Procedure; one limitation of the rule is, of course, the obligation to give a copy of the warrant and a receipt for the property taken “to the person from whom . . . the property was taken.” Fed. R. Crim. P. 41(f)(1)(C).

While not part of the SCA, a separate statute permits the notice thus required by Rule 41 to be delayed. 18 U.S.C. § 3103a(b). Therefore, as the government has done in its applications for warrants seeking geolocation data, and as the form permits, notification of the existence of a search warrant for an e-mail account can be delayed; however, it must ultimately be given. Under the SCA, contemporaneous notice of such a search need not be given to the subscriber of an e-mail account if the government seeks a

warrant under 18 U.S.C. §2703(b)(1)(A). The procedural terms of Rule 41, however, incorporated into the SCA, require that a copy of the warrant be given “to the person from whom . . . the property was taken.” Fed. R. Crim. P. 41(f)(1)(C). Notice, however, may be delayed according to 18 U.S.C. § 3103a(b).

The complication comes about when one realizes that the SCA contains its own authority for delaying notice of an order that the SCA itself authorizes. If probable cause to search an e-mail account is not available, the government may still get a court order requiring disclosure of the account, if the government nevertheless asserts “specific and articulable facts” showing reasonable grounds to believe that the contents of the account “are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). Once again, however, Congress requires that notice be ultimately given to a subscriber, but permits a delay in the required notice to the subscriber (as articulated in 18 U.S.C. § 2703(a)(1)(B)) if certain requirements (not pertinent here) are met. See 18 U.S.C. § 2705.

Read together, whether the government proceeds by seeking a search warrant, premised on probable cause, or by seeking a court order, premised on “specific and articulable facts,” notice must be given to the subscriber, but it may be delayed.

The only other way to read the pertinent provision of the SCA that provides that the government may secure a search warrant “without required notice” to the subscriber is to read it to dispense with the government’s ever being obliged to give notice to the subscriber. But, the subsection that seems to dispense with notice simultaneously requires that the government use the procedures in the Federal Rules of Criminal Procedure and one of those procedures is, unquestionably, the giving of notice, *i.e.*, the

leaving of a copy of the warrant and the receipt for what was taken. The plain text of the SCA therefore requires the very notice that the government seeks to avoid.

Further, the legislative history of the SCA indicates clearly that the purpose of the act was to address the expansion of opportunities for government intrusions created by the development of new methods of communication and devices for surveillance. S. Rep. No. 99-541, at 2 (1986). Accordingly, Congress asserted that “the law must advance with the technology to ensure the continued vitality of the fourth amendment . . . Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.” *Id.* at 5.

As such, note how carefully Congress has postponed the giving of notice of the disclosure of the contents of stored communications in the SCA itself and in 18 U.S.C. § 3103a. In § 3103a, a judicial officer may provide for delayed notice accordingly:

(b) Delay.— With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if —

(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial);

(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and

(3) the warrant provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay.

18 U.S.C. § 3103a. The text of subsection (b)(2) specifically refers to the SCA, which is “chapter 121,” and to stored wire and electronic communications. The SCA already provides for delayed notification of court orders and administrative subpoenas issued under § 2703(b) of the SCA. Thus, Congress had to have understood that the SCA and § 3103a would be read together to permit delay of notification of warrants issued under the SCA and Rule 41 of the Federal Rules of Criminal Procedure. Further, it only makes sense for Congress to have allowed for the delay of notification because it understood that notice was required to be given in the first place.

It can be said with confidence that Congress has never indicated that it considers the giving of notice as a mere formality. To the contrary, in this new world where the government can detect a person’s location by her cell phone signals and read her e-mails, Congress has required notice but permitted its postponement. Indeed, even a warrant for a tracking device must ultimately be given to the person who has been tracked. It is irrational to think that Congress would, in the teeth of that care, grant the government a perpetual dispensation from ever notifying a person of the remarkable intrusion that a search of his e-mail account creates. In fact, in discussing the amendments made to 18 U.S.C. § 3103a, the legislative history makes clear that changes were made to ensure that, when utilizing the so-called “sneak-and-peek” warrant under 18 U.S.C. § 3103a, the government was prohibited from seizing any wire or electronic communication, or any stored electronic information, without a showing of reasonable necessity, *and* that notice

of the search of the same be given within a reasonable time of the execution of the warrant. See, e.g., 147 Cong. Rec. S11,002 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

Finally, the government's claim that notice to the Internet Service Provider ("ISP") complies with the notice requirement is unpersuasive. Why does an ISP need notice, via a copy of the warrant, when it is being served with the warrant or order? It is inconceivable that Congress, which took such care in identifying when and how notice to the person whose privacy has been invaded is to be given, would dispense with those requirements because of the meaningless act of telling the ISP what it already knows. The legislative history of the SCA tells us that Congress was concerned with "protect[ing] the sanctity and privacy of the communication" and "afford[ing] protection against governmental snooping in these files." 132 Cong. Rec. 14,886 (1986) (statement of Rep. Kastenmeier). One such protection provided by Congress in the SCA and Rule 41 of the Federal Rules of Criminal Procedure is notice.

Thus, for the reasons stated herein, it is, hereby,

ORDERED that the government's motion for clarification is **GRANTED**. It is further, hereby,

ORDERED that this Memorandum Order shall serve as the clarification the government seeks and shall confirm that the government is required to provide notice to the subscriber of the e-mail being searched, pursuant to Rule 41(f)(1)(C). Such notice may be delayed, as Magistrate Judge Kay has provided, according to 18 U.S.C. § 3103a(b), and that period of delay may be extended upon motion to the Court for such

extension. Nevertheless, eventually, the subscriber of the e-mail account to be searched shall receive a copy of the warrant as notice, pursuant to Rule 41(f)(1)(C).

SO ORDERED.



Digitally signed by
John M. Facciola
Date: 2010.07.21
14:14:32 -04'00'

JOHN M. FACCIOLA
UNITED STATES MAGISTRATE JUDGE

EXHIBIT G

Other Orders/Judgments

1:10-mj-00291-AK *SEALED* USA v. E-MAIL ACCOUNT

██████████@GMAIL.COM ON COMPUTER SERVERS OPERATED BY
GOOGLE, INC., 1600 AMPHITHEATRE PARKWAY, MOUNTAIN VIEW, CALIFORNIA
CLOSED, Sealed_Case

U.S. District Court

District of Columbia

Notice of Electronic Filing

The following transaction was entered on 7/21/2010 at 2:55 PM and filed on 7/21/2010

USA v. E-MAIL ACCOUNT ██████████@GMAIL.COM ON COMPUTER
Case Name: SERVERS OPERATED BY GOOGLE, INC., 1600 AMPHITHEATRE PARKWAY,
MOUNTAIN VIEW, CALIFORNIA

**Case
Number:** 1:10-mj-00291-AK *SEALED*

Filer:

**Document
Number:** No document attached

Docket Text:

MINUTE ORDER as to E-MAIL ACCOUNT ██████████@GMAIL.COM ON
COMPUTER SERVERS OPERATED BY GOOGLE, INC., 1600 AMPHITHEATRE PARKWAY,
MOUNTAIN VIEW, CALIFORNIA: MINUTE ORDER: I have issued a Memorandum Order
regarding the government's motion for clarification. I have filed the Memorandum Order
under seal; however, the Order to Seal issued in this case by Magistrate Judge Kay
does not extend to my Memorandum Order. Thus, the government is hereby ORDERED
to show cause in writing within five days of this order why I should not unseal the
Memorandum Order for public view. The unsealed version of the Memorandum Order
would be subject to the redaction of the e-mail address at issue in the case and any
language that would identify the e-mail address or topic of the investigation. SO
ORDERED. Signed by Magistrate Judge John M. Facciola on 07/21/10. (zldc,)

1:10-mj-00291-AK *SEALED*-1 No electronic public notice will be sent because the case/entry is
sealed.

EXHIBIT H

**THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

**APPLICATION FOR SEARCH WARRANT)
FOR E-MAIL ACCOUNT)
[REDACTED]@GMAIL.COM)
MAINTAINED ON COMPUTER SERVERS)
OPERATED BY GOOGLE, INC.,)
HEADQUARTERED AT)
1600 AMPHITHEATRE PARKWAY,)
MOUNTAIN VIEW, CA)**

Mag. No.: 10-291-M-01(AK/JMF)

UNDER SEAL

FILED

JUL 23 2010

**Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia**

**MOTION TO VACATE MEMORANDUM ORDER AND, IN THE ALTERNATIVE, FOR
RECONSIDERATION, AND TO STAY UNSEALING PENDING FURTHER REVIEW**

On July 21, 2010, this Court, acting through Magistrate Judge John M. Facciola, entered a Memorandum Order adjudicating the Government's Motion for Clarification of Notice Obligations for E-mail Search Warrant ("Motion for Clarification") in this matter. Prior to the issuance of that Memorandum Order, however, this Court, acting through Magistrate Judge Alan Kay, had already received, reviewed, considered, and acted on the Government's Motion for Clarification. For this reason, the Government respectfully requests that the Court vacate its July 21, 2010 Memorandum Order. In the alternative, the Government asks the Court to reconsider its July 21, 2010, Memorandum Order. Finally, the Government requests that the Order, the proceedings, this pleading and all other filings in this case, remain under seal pending any further review of the Order by the Court, to include, as necessary, review by the Chief Judge of the District Court.

I. The July 21, 2010 Memorandum Order Should Be Vacated

Magistrate Judge Facciola's July 21, 2010, Memorandum Order considering the Government's Motion for Clarification should be vacated because the Government's motion was already considered and adjudicated by Magistrate Judge Kay one month earlier. In issuing its July 21, 2010 Memorandum Order, the Court was likely unaware of some of the following pertinent facts:

X

UNDER SEAL

On May 28, 2010, the Government applied for a warrant to search certain contents of the [REDACTED]@gmail.com account. As the presiding Magistrate Judge handling warrants in May, Magistrate Judge Kay reviewed and issued the warrant. In so doing, Magistrate Judge Kay checked the box on the face of the warrant allowing for delayed notification under 18 U.S.C. § 3103a. The Government had not requested such relief in its search warrant application. On June 8, 2010, the Government filed a Motion for Clarification seeking to clarify Magistrate Judge Kay's intent in checking the box. As the Motion for Clarification related directly to the [REDACTED]@gmail.com search warrant and Magistrate Judge Kay's actions thereon, the Government submitted its motion with the same caption and case number as the warrant (i.e., Mag. No. 10-291-M-01(AK)). Consistent with Local Criminal Rule 57.10(c), the Government's Motion was properly considered and acted on by Magistrate Judge Kay. See LCrR57.10(c) ("All proceedings in a case after its assignment shall be conducted by the judge to whom the case is assigned, except as otherwise provided in these Rules.").

Specifically, on June 17, 2010, having received and reviewed the Government's Motion for Clarification, and upon learning that the undersigned Assistant United States Attorney who had filed the Motion was out of the office on leave, Magistrate Judge Kay contacted Gregg A. Maisel, the then-Acting Chief of the National Security Section of the United States Attorney's Office. When they spoke, Magistrate Judge Kay indicated that he had checked the box on the face of the warrant in error and believed that the law was clear that the Government had no notice obligation for the warrant regardless of whether or not the issuing judge checked the box on the face of the warrant permitting delayed notice under 18 U.S.C. § 3103a. Magistrate Judge Kay asked Acting Chief Maisel how he proposed the Court to proceed, to which Acting Chief Maisel responded by inquiring

UNDER SEAL

if the Court had received a proposed order accompanying the Government's Motion. Magistrate Judge Kay indicated that he had not seen any proposed order,¹ and he also indicated that he believed the issuance of a separate written order on the Government's Motion was unnecessary. Rather, Magistrate Judge Kay indicated that the United States Attorney's Office should submit a copy of the warrant with his original signature, and that he would then correct the face of the warrant and return it to this Office for its files. On June 21, 2010, having located a copy of the warrant with an original signature, Acting Chief Maisel re-contacted Magistrate Judge Kay to inform him that he would have the warrant delivered to chambers. Magistrate Judge Kay indicated that he had corrected (or would correct) the face of the copy of the warrant in the Court's file. Pursuant to Magistrate Judge Kay's direction, on June 21, 2010, Acting Chief Maisel returned the original warrant to Magistrate Judge Kay "for further clarifying annotation." See Exhibit A hereto. Magistrate Judge Kay then marked "checked in error AK" next to the delayed notification provision, and returned the warrant to the United States Attorney's Office for its files. See id.

In sum, Magistrate Judge Kay received, reviewed, considered, and acted on the Government's Motion for Clarification one month prior to the issuance of the July 21, 2010, Memorandum Order. Accordingly, the latter order should be vacated as improvidently issued.

II. Alternatively, the July 21, 2010 Memorandum Order Should Be Reconsidered

The Government does not seek to belabor the point here² but respectfully requests that, if the

¹ The Government had filed a proposed order, but it inadvertently was not included in Magistrate Judge Kay's chamber's copy of the Government's Motion.

² The Government recognizes that the Court addressed in its July 21, 2010 Memorandum Order legal principles of broad applicability that the Court will likely have occasion to address again in other matters in the near future.

UNDER SEAL

July 21, 2010 Memorandum Order is not vacated, the Order be reconsidered in light of the following:

- The Order's conclusion that a warrant issued pursuant to the Stored Communications Act ("SCA") requires notice to an e-mail account subscriber or customer is contrary to the plain language of 18 U.S.C. § 2703(b)(1)(A), as other courts have so found. See, e.g., Guest v. Leis, 255 F.3d 325, 338-39 n. 7 (6th Cir. 2001); Bansal v. Russ, 513 F. Supp. 2d 264, 276-77 (E.D. Pa. 2007).
- The Order erred in concluding that Fed. R. Crim. P. 41(f)'s provisions regarding the *execution* and *return* of a warrant are incorporated into section 18 U.S.C. § 2703(b)(1)(A) by virtue of its limitation that a warrant thereunder must be "*issued* using the procedures described in the Federal Rules of Criminal Procedure." 18 U.S.C. § 2703(b)(1)(A) (emphasis added). By its own terms the latter phrase incorporates only those procedural portions of Rule 41 related to the *issuance* of the warrant (*i.e.*, Rule 41(d) and (e)), not to procedures related to the execution and return of the warrant, *i.e.*, the entirety of Rule 41(f). See United States v. Berkos, 543 F.3d 392, 398 (7th Cir. 2008) ("Section 2703(a) refers only to the specific provision of the Rules of Criminal Procedure, namely, Rule 41, that detail the *procedures* for obtaining and issuing warrants.") (emphasis in original); In re Search of Yahoo, Inc., No. 07-3194-MB, 2007 WL 1539971 at *6 (D. Ariz. May 21, 2007) (unpublished); and In re Search Warrant, No. 6:05-MC-168-Orl-31JGG, 2005 WL 3844032 at *5-6 (M.D. Fla. Feb. 13, 2006) (unpublished). But see In the Matter of the Application of the United States of America for a Search Warrant, 665 F. Supp. 2d 1210, 1219 (D. Or. 2009). Rule 41(f) describes steps the officer executing the warrant should take such as noting the time of execution, inventorying property seized, providing a receipt, and making a prompt return of the warrant. Fed. R. Crim. P. 41(f). These steps have nothing to do with the *issuance* of a warrant and would, in any event, be out of place in the SCA which does not even require that an officer be present when such a warrant is executed. See 18 U.S.C. § 2703(g).
- The Order erred in concluding that providing a receipt and notice to an Internet Service Provider ("ISP") would not satisfy the requirements of Fed. R. Crim. P. 41(f)(1)(C). When the Government executes a search warrant on the premises of a third-party, it satisfies the requirements of Rule 41(f)(1)(C) by giving the third-party "from whose premises . . . the property was taken" a copy of the warrant. See, e.g., United States v. Zacher, 465 F.3d 336, 339 (8th Cir. 2006). Serving a SCA warrant on an ISP satisfies that requirement. See In the Matter of the Application of the United States of America for a Search Warrant, 665 F. Supp. 2d at 1221-22. There is not, and never has been, a requirement under Rule 41(f) to give notice to the criminal suspect who may have an interest in property seized from a third party. See id.

UNDER SEAL

III. The July 21, 2010 Memorandum Order Should Remain Sealed Pending Review

Because the July 21, 2010, Memorandum Order should be vacated, it should not be unsealed. For the same reason, if the Government's motion to vacate is denied, the Government respectfully requests that the Memorandum Order, the proceedings, this pleading and all other filings in this case, remain under seal pending any further review of the Order by the Court, to include, as necessary, review by the Chief Judge of the District Court. See Fed. R. Crim. P. 1(c); LCvR 40.7(g); LCrR 57.17(a).

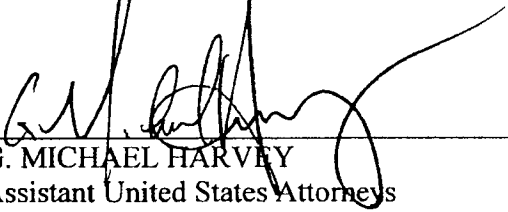
IV. Conclusion

Wherefore, the Government respectfully requests that the Court vacate its July 21, 2010 Memorandum Order or, in the alternative, reconsider it. Additionally, in the event that the Court denies the Government's motion to vacate the Order, the Government respectfully requests that the Order remain under seal pending further review of that Order by the Chief Judge of the District Court. A proposed Order is attached.

Respectfully submitted,


RONALD G. MACHEN JR.
UNITED STATES ATTORNEY

By:



G. MICHAEL HARVEY
Assistant United States Attorneys
D.C. Bar Number 447-465
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-439
Washington, D.C. 20530
Phone: (202) 305-4155
Michael.Harvey2@usdoj.gov

UNDER SEAL



JONATHAN M. MALIS
Assistant United States Attorney
D.C. Bar Number 454-548
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-447
Washington, D.C. 20530
Phone: (202) 305-9665
Jonathan.M.Malis@usdoj.gov

Dated: July 23, 2010

EXHIBIT A



U.S. Department of Justice

Ronald C. Machen Jr.
United States Attorney

District of Columbia

*Judiciary Center
555 Fourth St., N.W.
Washington, D.C. 20530*

June 21, 2010

The Honorable Alan Kay
U.S. Magistrate Judge for the
District of Columbia
Washington, D.C.

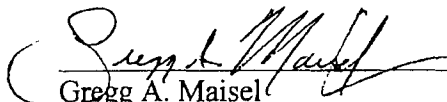
Re: In the Matter of the Search of the E-Mail Account [REDACTED]@gmail.com
Case No. 10-291-M-01

Dear Judge Kay:

Per our discussion and your request, I am returning the original Search and Seizure
Warrant in the above-referenced matter for further clarifying annotation.

Feel free to contact me at (202) 514-7746 if you would like to discuss this matter further.
Thank you.

Sincerely,



Gregg A. Maisel
Acting Chief
National Security Section

Enclosure

UNITED STATES DISTRICT COURT

for the
District of ColumbiaIn the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))

Case No. 10-291-M-01

E-mail Account [REDACTED]@gmail.com on)
Computer Servers Operated by Google, Inc., 1600)
Amphitheatre Parkway, Mountain View, California)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California

(Identify the person or describe the property to be searched and give its location):

E-mail account [REDACTED]@gmail.com, maintained on computer servers operated by Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the property to be seized):

Certain property, the disclosure of which is governed by Title 42, U.S.C. Section 2000aa, and Title 18, U.S.C. Sections 2701 through 2711, namely contents of electronic e-mails and other electronic data, more fully described in ATTACHMENT A to this application.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before

JUN 11 2010

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

(name)

I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☒ for 30 days (not to exceed 30).☐ until, the facts justifying, the later specific date of

Date and time issued: MAY 28 2010

City and state: District of Columbia

ALAN RA
U.S. MAGISTRATE JUDGE

Printed name and title

checked in error

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized: 		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <p>Date: _____ _____ <i>Executing officer's signature</i> _____ <i>Printed name and title</i></p>		

UNDER SEAL

on that same date. When signing the warrant, Magistrate Judge Kay checked the box on the front of the warrant indicating that the Court found that immediate notification of the warrant “to the person who, or whose property, will be searched or seized” would “have an adverse result listed in 18 U.S.C. § 2705” and permitted delayed notification for up to 30 days. Believing it had no obligation under the law to notify the subscriber or customer of the e-mail account concerning the warrant, the Government had not requested such relief from the Court in its search warrant application. On June 8, 2010, the Government filed a Motion for Clarification seeking to clarify Magistrate Judge Kay’s intent in checking the box. Thereafter, consistent with Local Criminal Rule 57.10(c), the Government’s Motion was properly considered and acted on by Magistrate Judge Kay. See LCrR57.10(c) (“All proceedings in a case after its assignment shall be conducted by the judge to whom the case is assigned, except as otherwise provided in these Rules.”).²

² Specifically, on June 17, 2010, having received and reviewed the Government’s Motion for Clarification, and upon learning that the undersigned Assistant United States Attorney who had filed the Motion was out of the office on leave, Magistrate Judge Kay contacted Gregg A. Maisel, the then-Acting Chief of the National Security Section of the United States Attorney’s Office. When they spoke, Magistrate Judge Kay indicated that he had checked the box on the face of the warrant in error and believed that the law was clear that the Government had no notice obligation for the warrant regardless of whether or not the issuing judge checked the box on the face of the warrant delaying notice. Magistrate Judge Kay asked Acting Chief Maisel how he proposed the Court to proceed, to which Acting Chief Maisel responded by inquiring if the Court had received a proposed order accompanying the Government’s Motion. Magistrate Judge Kay indicated that he had not seen any proposed order, and he also indicated that he believed the issuance of a separate written order on the Government’s Motion was unnecessary. Rather, Magistrate Judge Kay indicated that the United States Attorney’s Office should submit a copy of the warrant with his original signature, and that he would then correct the face of the warrant and return it to this Office for its files. On June 21, 2010, having located a copy of the warrant with an original signature, Acting Chief Maisel re-contacted Magistrate Judge Kay to inform him that he would have the warrant delivered to chambers. Magistrate Judge Kay indicated that he had corrected (or would correct) the face of the copy of the warrant in the Court’s file. Pursuant to Magistrate Judge Kay’s direction, on June 21, 2010, Acting Chief

UNDER SEAL

Presumably unaware of Magistrate Judge Kay's adjudication of the Government's Motion for Clarification, on July 21, 2010, this Court, acting through Magistrate Judge John M. Facciola, entered a Memorandum Order also adjudicating the Government's Motion for Clarification. Because its motion had already been adjudicated by Magistrate Judge Kay, on July 23, 2010, the Government filed a motion to vacate, or in the alternative, for reconsideration of the July 21, 2010 Memorandum Order ("Motion to Vacate") and served courtesy copies of the same on both Magistrate Judge Facciola and Magistrate Judge Kay. In its motion to vacate, the Government also sought, in the alternative, for reconsideration of the July 21, 2010, Memorandum Order and to stay unsealing of that order pending its further reviewed by the Chief Judge of the District Court.

As of the date of the filing of this motion for enlargement, the Government's Motion to Vacate had not been adjudicated by either Magistrate Judge Facciola or Magistrate Judge Kay. Federal Rule of Criminal Procedure 59(a) requires that written objections to a nondispositive order of a Magistrate Judge be filed within 14 days after service of the order in question. The July 21, 2010 Order was received by the Government by fax on July 21, 2010. Federal Rule of Criminal Procedure 59(a) does not address the present scenario where the Government has filed a motion with the Magistrate Judge seeking to vacate or, in the alternative, for reconsideration of the Magistrate Judge's order. Adjudication of the pending Motion to Vacate by the Magistrate Judge may resolve the issue without need of further review by Chief Judge. Therefore, to preserve judicial resources, and in an abundance of caution, the Government seeks an

Maisel returned the original warrant to Magistrate Judge Kay "for further clarifying annotation." Magistrate Judge Kay then marked "checked in error AK" next to the delayed notification provision, and returned the warrant to the United States Attorney's office for its files.

UNDER SEAL

enlargement of time under Federal Rule of Criminal Procedure 59(a) to file objections to the July 21, 2010 Order until 14 days after adjudication of the Government's motion presently pending before the Magistrate Judge seeking to vacate, or in the alternative, for reconsideration of the July 21, 2010 Order.

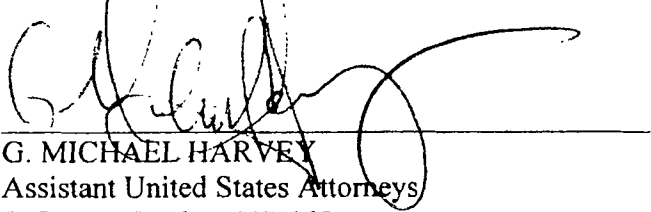
Further, because the Government believes that the July 21, 2010 Order should properly be vacated, it respectfully requests that the July 21, 2010 Order, its Motion to Vacate, this motion and order, and any adjudication of the Government's pending Motion to Vacate by the Magistrate Judge, remain under seal pending further order of the Chief Judge of this Court.

Wherefore, the Government respectfully requests that this Court grant this motion for an enlargement of time permitting the Government to file any objections to the July 21, 2010 Order within 14 days of the adjudication of its Motion to Vacate by the Magistrate Judge. Further, the Government respectfully requests that the July 21, 2010 Order, and any adjudication of the Government's pending Motion to Vacate by the Magistrate Judge, remain under seal pending further order of the Chief Judge of this Court. A proposed Order is attached.

Respectfully submitted,

RONALD G. MACHEN JR.
UNITED STATES ATTORNEY

By:



G. MICHAEL HARVEY
Assistant United States Attorneys
D.C. Bar Number 447-465
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-439
Washington, D.C. 20530
Phone: (202) 305-4155

UNDER SEAL

Michael.Harvey2@usdoj.gov



JONATHAN M. MALIS

Assistant United States Attorney

D.C. Bar Number 454-548

National Security Section

United States Attorney's Office

555 4th Street, N.W., Room 11-447

Washington, D.C. 20530

Phone: (202) 305-9665

Jonathan.M.Malis@usdoj.gov

Dated: August 4, 2010

EXHIBIT I

FILED4 MLP
AUG 09 2010THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF COLUMBIAClerk U.S. District & Bankruptcy
Courts for the District of Columbia

APPLICATION FOR SEARCH WARRANT)
 FOR E-MAIL ACCOUNT) **Mag. No.: 10-291-M-01**
 [REDACTED]@GMAIL.COM) **(AK/JMF/RCL)**
 MAINTAINED ON COMPUTER SERVERS)
 OPERATED BY GOOGLE, INC.,) **UNDER SEAL**
 HEADQUARTERED AT)
 1600 AMPHITHEATRE PARKWAY,)
 MOUNTAIN VIEW, CA)

**GOVERNMENT'S MOTION FOR ENLARGEMENT OF TIME TO FILE OBJECTIONS
 TO JULY 21, 2010 MEMORANDUM ORDER OF MAGISTRATE JUDGE AND TO
STAY UNSEALING PENDING FURTHER ORDER OF THE CHIEF JUDGE**

The United States, by and through the United States Attorney for the District of Columbia, respectfully requests the Chief Judge of this Court to enlarge the time under Federal Rule of Criminal Procedure 59(a)¹ to file objections to the Magistrate Judge's July 21, 2010 Memorandum Order in this matter ("July 21, 2010 Order") until 14 days after adjudication of the Government's motion presently pending before the Magistrate Judge seeking to vacate, or in the alternative, for reconsideration of that order ("Motion to Vacate"). Further, the Government respectfully requests that the July 21, 2010 Order, and any adjudication of the Government's pending Motion to Vacate by the Magistrate Judge, remain under seal pending further order of the Chief Judge of this Court.

There is good cause for this motion. On May 28, 2010, the Government applied for a warrant to search the contents of Google, Inc., e-mail account [REDACTED]@gmail.com. The Court, acting through Magistrate Judge Alan Kay, granted the request and issued the warrant

¹ Federal Rule of Criminal Procedure 59(a) permits the filing of objections to a Magistrate Judge's non-dispositive order "within 14 days after being served with a copy of the written order . . . or at some other time the court sets." F.R.Cr.P. 59(a)(emphasis added); see also Thomas v. Arn, 474 U.S. 140, 155 (1985) (allowing for a rule conditioning appeal from a Magistrate Judge's order upon the filing of objections to that order with the District Court, provided that the rule incorporates "clear notice to the litigants and an opportunity to seek an extension of time for filing objections").

8

UNDER SEAL

on that same date. When signing the warrant, Magistrate Judge Kay checked the box on the front of the warrant indicating that the Court found that immediate notification of the warrant “to the person who, or whose property, will be searched or seized” would “have an adverse result listed in 18 U.S.C. § 2705” and permitted delayed notification for up to 30 days. Believing it had no obligation under the law to notify the subscriber or customer of the e-mail account concerning the warrant, the Government had not requested such relief from the Court in its search warrant application. On June 8, 2010, the Government filed a Motion for Clarification seeking to clarify Magistrate Judge Kay’s intent in checking the box. Thereafter, consistent with Local Criminal Rule 57.10(c), the Government’s Motion was properly considered and acted on by Magistrate Judge Kay. See LCrR57.10(c) (“All proceedings in a case after its assignment shall be conducted by the judge to whom the case is assigned, except as otherwise provided in these Rules.”).²

² Specifically, on June 17, 2010, having received and reviewed the Government’s Motion for Clarification, and upon learning that the undersigned Assistant United States Attorney who had filed the Motion was out of the office on leave, Magistrate Judge Kay contacted Gregg A. Maisel, the then-Acting Chief of the National Security Section of the United States Attorney’s Office. When they spoke, Magistrate Judge Kay indicated that he had checked the box on the face of the warrant in error and believed that the law was clear that the Government had no notice obligation for the warrant regardless of whether or not the issuing judge checked the box on the face of the warrant delaying notice. Magistrate Judge Kay asked Acting Chief Maisel how he proposed the Court to proceed, to which Acting Chief Maisel responded by inquiring if the Court had received a proposed order accompanying the Government’s Motion. Magistrate Judge Kay indicated that he had not seen any proposed order, and he also indicated that he believed the issuance of a separate written order on the Government’s Motion was unnecessary. Rather, Magistrate Judge Kay indicated that the United States Attorney’s Office should submit a copy of the warrant with his original signature, and that he would then correct the face of the warrant and return it to this Office for its files. On June 21, 2010, having located a copy of the warrant with an original signature, Acting Chief Maisel re-contacted Magistrate Judge Kay to inform him that he would have the warrant delivered to chambers. Magistrate Judge Kay indicated that he had corrected (or would correct) the face of the copy of the warrant in the Court’s file. Pursuant to Magistrate Judge Kay’s direction, on June 21, 2010, Acting Chief

UNDER SEAL

Presumably unaware of Magistrate Judge Kay's adjudication of the Government's Motion for Clarification, on July 21, 2010, this Court, acting through Magistrate Judge John M. Facciola, entered a Memorandum Order also adjudicating the Government's Motion for Clarification. Because its motion had already been adjudicated by Magistrate Judge Kay, on July 23, 2010, the Government filed a motion to vacate, or in the alternative, for reconsideration of the July 21, 2010 Memorandum Order ("Motion to Vacate") and served courtesy copies of the same on both Magistrate Judge Facciola and Magistrate Judge Kay. In its motion to vacate, the Government also sought, in the alternative, for reconsideration of the July 21, 2010, Memorandum Order and to stay unsealing of that order pending its further reviewed by the Chief Judge of the District Court.

As of the date of the filing of this motion for enlargement, the Government's Motion to Vacate had not been adjudicated by either Magistrate Judge Facciola or Magistrate Judge Kay. Federal Rule of Criminal Procedure 59(a) requires that written objections to a nondispositive order of a Magistrate Judge be filed within 14 days after service of the order in question. The July 21, 2010 Order was received by the Government by fax on July 21, 2010. Federal Rule of Criminal Procedure 59(a) does not address the present scenario where the Government has filed a motion with the Magistrate Judge seeking to vacate or, in the alternative, for reconsideration of the Magistrate Judge's order. Adjudication of the pending Motion to Vacate by the Magistrate Judge may resolve the issue without need of further review by Chief Judge. Therefore, to preserve judicial resources, and in an abundance of caution, the Government seeks an

Maisel returned the original warrant to Magistrate Judge Kay "for further clarifying annotation." Magistrate Judge Kay then marked "checked in error AK" next to the delayed notification provision, and returned the warrant to the United States Attorney's office for its files.

UNDER SEAL

enlargement of time under Federal Rule of Criminal Procedure 59(a) to file objections to the July 21, 2010 Order until 14 days after adjudication of the Government's motion presently pending before the Magistrate Judge seeking to vacate, or in the alternative, for reconsideration of the July 21, 2010 Order.

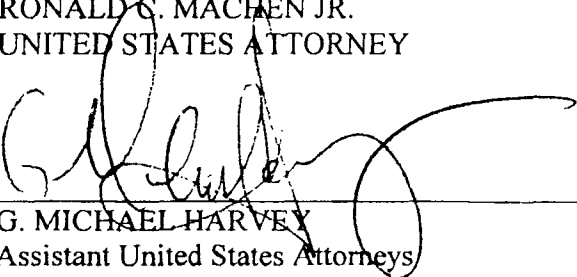
Further, because the Government believes that the July 21, 2010 Order should properly be vacated, it respectfully requests that the July 21, 2010 Order, its Motion to Vacate, this motion and order, and any adjudication of the Government's pending Motion to Vacate by the Magistrate Judge, remain under seal pending further order of the Chief Judge of this Court.

Wherefore, the Government respectfully requests that this Court grant this motion for an enlargement of time permitting the Government to file any objections to the July 21, 2010 Order within 14 days of the adjudication of its Motion to Vacate by the Magistrate Judge. Further, the Government respectfully requests that the July 21, 2010 Order, and any adjudication of the Government's pending Motion to Vacate by the Magistrate Judge, remain under seal pending further order of the Chief Judge of this Court. A proposed Order is attached.

Respectfully submitted,

RONALD G. MACHEN JR.
UNITED STATES ATTORNEY

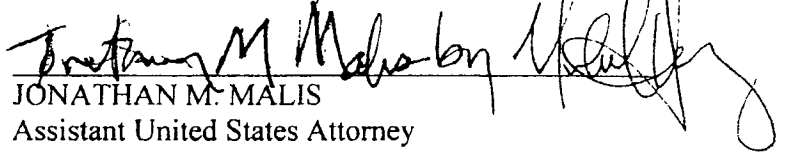
By:



G. MICHAEL HARVEY
Assistant United States Attorneys
D.C. Bar Number 447-465
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-439
Washington, D.C. 20530
Phone: (202) 305-4155

UNDER SEAL

Michael.Harvey2@usdoj.gov

A handwritten signature in black ink, appearing to read "Jonathan M. Malis", is written over a horizontal line.

JONATHAN M. MALIS

Assistant United States Attorney

D.C. Bar Number 454-548

National Security Section

United States Attorney's Office

555 4th Street, N.W., Room 11-447

Washington, D.C. 20530

Phone: (202) 305-9665

Jonathan.M.Malis@usdoj.gov

Dated: August 4, 2010

EXHIBIT J

THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT)
FOR E-MAIL ACCOUNT)
[REDACTED]@GMAIL.COM)
MAINTAINED ON COMPUTER SERVERS)
OPERATED BY GOOGLE, INC.,)
HEADQUARTERED AT)
1600 AMPHITHEATRE PARKWAY,)
MOUNTAIN VIEW, CA)

Mag. No.: 10-291-M-01
(AK/JMF/RCL)

UNDER SEAL

FILED

AUG - 5 2010

~~PROPOSED~~ ORDER

Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

Having reviewed the Government's Motion for Enlargement of Time to File Objections to July 21, 2010 Memorandum Order of Magistrate Judge and to Stay Unsealing Pending Further Order of the Chief Judge ("Motion for Enlargement"), it is this 5th day of August 2010, hereby

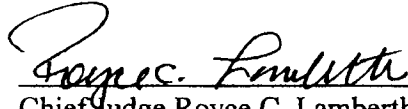
ORDERED that the Government's Motion for Enlargement is **GRANTED**; and it is

FURTHER ORDERED that the Government has until 14 days from the service of the Magistrate Judge's adjudication of its Motion to Vacate Memorandum Order and, in the Alternative, For Reconsideration, and to Stay Unsealing Pending Further Review ("Motion to Vacate"), to file objections to the Magistrate Judge's July 21, 2010 Memorandum Order in this matter; and it is

FURTHER ORDERED the July 21, 2010 Memorandum Order, the Government's Motion to Vacate, the present Motion for Enlargement, this Order, and any adjudication of the Government's pending Motion to Vacate by the Magistrate Judge, remain under seal pending further order of the Chief Judge of this Court.

(N)

9



Chief Judge Royce C. Lamberth
United States District Court
for the District of Columbia

copied to:

G. Michael Harvey
Jonathan M. Malis
Assistant United States Attorneys
United States Attorney's Office
555 4th Street, N.W., 11th Floor
Washington, D.C. 20530

EXHIBIT K

MIME-Version:1.0
 From:DCD_ECFNotice@dcd.uscourts.gov
 To:DCD_ECFNotice@localhost.localdomain
 Bcc:
 --Case Participants:
 --Non Case Participants:
 --No Notice Sent:

Message-Id:<2652348@dcd.uscourts.gov>
 Subject:Activity in Case 1:10-mj-00291-AK *SEALED* USA v. E-MAIL ACCOUNT
 [REDACTED]@GMAIL.COM ON COMPUTER SERVERS OPERATED BY GOOGLE, INC.,
 1600 AMPHITHEATRE PARKWAY, MOUNTAIN VIEW, CALIFORNIA Order on Motion to Vacate
 Content-Type: text/html

This is an automatic e-mail message generated by the CM/ECF system. Please DO NOT RESPOND to this e-mail because the mail box is unattended.

*****NOTE TO PUBLIC ACCESS USERS***** Judicial Conference of the United States policy permits attorneys of record and parties in a case (including pro se litigants) to receive one free electronic copy of all documents filed electronically, if receipt is required by law or directed by the filer. PACER access fees apply to all other users. To avoid later charges, download a copy of each document during this first viewing. However, if the referenced document is a transcript, the free copy and 30 page limit do not apply.

NOTE: This docket entry (or case) is SEALED. Do not allow it to be seen by unauthorized persons.

U.S. District Court

District of Columbia

Notice of Electronic Filing

The following transaction was entered on 8/23/2010 at 6:01 PM and filed on 8/23/2010

Case Name: USA v. E-MAIL ACCOUNT [REDACTED]@GMAIL.COM ON COMPUTER
 SERVERS OPERATED BY GOOGLE, INC., 1600 AMPHITHEATRE PARKWAY,
 MOUNTAIN VIEW, CALIFORNIA

Case Number: 1:10-mj-00291-AK *SEALED*

Filer:

Document Number: No document attached

Docket Text:

MINUTE ORDER denying [7] Motion to Vacate: Having consulted with Magistrate Judge Kay on his decision to check the box delaying notification, I understand now that he believed the Government would still provide notice to the subscriber, regardless of whether it was delayed. In fact, upon the request of an Assistant United States Attorney, he withdrew the delayed notice; however, he believed the result in doing so would be that

the Government would notify the subscriber without any delay. Thus, he agrees with the analysis in my memorandum order and has authorized me to so state. Accordingly, seeing no grounds on which to vacate my order, it is hereby ORDERED that the motion to vacate is DENIED. It is further hereby ORDERED that the Government's motion to stay the unsealing of the memorandum order pending resolution of any appeal of that order to the Chief Judge is GRANTED. SO ORDERED. Signed by Magistrate Judge John M. Facciola on 08/23/2010. (lcjmf1)

1:10-mj-00291-AK *SEALED*-1 No electronic public notice will be sent because the case/entry is sealed.

EXHIBIT L

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR WARRANT)
FOR E-MAIL ACCOUNT)
[REDACTED]@GMAIL.COM)
MAINTAINED ON COMPUTER SERVERS)
OPERATED BY GOOGLE, INC.,)
HEADQUARTERED AT)
1600 AMPHITHEATRE PARKWAY,)
MOUNTAIN VIEW, CA)

Mag. No.: 10-291-M-01
(AK/JMF/RCL)

UNDER SEAL

FILED

SEP - 3 2010

Clerk, U.S. District Court for the District of Columbia

**MOTION FOR REVIEW OF MAGISTRATE JUDGE'S JULY 21, 2010
MEMORANDUM ORDER REGARDING NOTICE OBLIGATIONS
FOR E-MAIL WARRANTS ISSUED UNDER ECPA**

The United States, by and through the United States Attorney for the District of Columbia, respectfully requests, pursuant to Federal Rules of Criminal Procedure 1(c) and 59(a), as well as Local Civil Rule 40.7(g) and Local Criminal Rule 57.17(a), the review by the Chief Judge of this Court of the Magistrate Judge's July 21, 2010 Memorandum Order ("Mem. Order") in this matter, and states further as follows:

I. BACKGROUND

On May 28, 2010, pursuant to the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2710 ("ECPA"), the Government applied for a warrant to compel the disclosure of certain limited contents of the e-mail account [REDACTED]@gmail.com, which was maintained by Google, Inc. As the presiding Magistrate Judge handling warrants in May, Magistrate Judge Alan Kay reviewed and issued the warrant. In so doing, Magistrate Judge Kay checked the box on the face of the new warrant form issued this year by the Administrative Office of the United States Courts allowing for delayed notification under 18 U.S.C. § 3103a.¹ The Government had not requested such relief in its ECPA warrant application. On June 8, 2010, the Government

¹ The prior search warrant form used by this Court had no such delayed notification provision on the face of the form.

UNDER SEAL

filed a Motion for Clarification that sought to clarify Magistrate Judge Kay's intent in checking the box.

On July 21, 2010, Magistrate Judge John M. Facciola, entered a Memorandum Order adjudicating the Government's Motion for Clarification. See July 21, 2010 Memorandum Order ("Mem. Order") attached as Exhibit A hereto. In his Memorandum Order, Magistrate Judge Facciola held that the Government was obligated to notify the subscriber or customer of the e-mail account that was the subject of the ECPA warrant. Mem. Order at 11. Believing its Motion for Clarification had already been adjudicated by Magistrate Judge Kay,² on July 23, 2010, the Government filed a motion to vacate, or in the alternative, for reconsideration of Magistrate Judge Facciola's July 21, 2010 Memorandum Order ("Motion to Vacate"). In its Motion to Vacate, the Government also sought an order staying the unsealing of the

² On June 17, 2010, having received and reviewed the Government's Motion for Clarification, and upon learning that the undersigned Assistant United States Attorney who had filed the Motion was out of the office on leave, Magistrate Judge Kay contacted Gregg A. Maisel, the (then-Acting) Chief of the National Security Section of the United States Attorney's Office. When they spoke, Magistrate Judge Kay indicated that he had checked the box on the face of the warrant in error and believed that the law was clear that the Government had no notice obligation for the warrant regardless of whether or not the issuing judge checked the box on the face of the warrant permitting delayed notice under 18 U.S.C. § 3103a. Magistrate Judge Kay indicated that he believed the issuance of a separate written order on the Government's Motion was unnecessary. Rather, Magistrate Judge Kay indicated that the United States Attorney's Office should submit a copy of the warrant with his original signature, and that he would then correct the face of the warrant and return it to this Office for its files. On June 21, 2010, Chief Maisel re-contacted Magistrate Judge Kay to inform him that he would have the warrant delivered to chambers. Magistrate Judge Kay indicated that he had corrected (or would correct) the face of the copy of the warrant in the Court's file. Pursuant to Magistrate Judge Kay's direction, on June 21, 2010, Chief Maisel returned the original warrant to Magistrate Judge Kay "for further clarifying annotation." Magistrate Judge Kay then marked "checked in error AK" next to the delayed notification provision, and returned the warrant to the United States Attorney's Office for its files.

UNDER SEAL

Memorandum Order pending adjudication of the Motion to Vacate and its further review, if necessary, by this Court.

On August 4, 2010, its Motion to Vacate not having been adjudicated, the Government sought an enlargement of time to seek review of the Memorandum Order by the Chief Judge of this Court until 14 days after service of the Magistrate Judge's adjudication of the Government's Motion to Vacate the Memorandum Order. On August 5, 2010, this Court granted that motion. This Court also granted the Government's request that the Memorandum Order, Motion to Vacate, Motion for Enlargement, and any adjudication by the Magistrate Judge of the Government's Motion to Vacate remain sealed pending further review by the Chief Judge.

On August 23, 2010, the Government was served with Magistrate Judge Facciola's Minute Order denying its Motion to Vacate. See August 23, 2010 Minute Order attached as Exhibit B hereto. In that order, Magistrate Judge Facciola stated:

Having consulted with Magistrate Judge Kay on his decision to check the box delaying notification, I understand now that he believed the Government would still provide notice to the subscriber, regardless of whether it was delayed. In fact, upon the request of an Assistant United States Attorney, he withdrew the delayed notice; however, he believed the result in doing so would be that the Government would notify the subscriber without delay. Thus, he agrees with the analysis in my memorandum order and has authorized me to so state. Accordingly, seeing no grounds on which to vacate my order, it is hereby ORDERED that the motion to vacate is DENIED.

See id.³ Based on the above representations of Magistrate Judge Facciola, the Government does not seek further review of the denial of its Motion to Vacate. It does, however, seek review and reversal of Magistrate Judge Facciola's Memorandum Order on the merits.

³ In the Minute Order, Magistrate Judge Facciola also granted the Government's request that the unsealing of the Memorandum Order be stayed pending resolution of any review of that order by the Chief Judge. See id.

UNDER SEAL

Indeed, whether the Government is obligated to notify the subscriber or customer of an e-mail account that is the subject of compelled disclosure pursuant to an ECPA warrant is a question of broad applicability. The Department of Justice has always read the plain language of ECPA as not requiring notice to the customer or subscriber of the e-mail account at issue. Following that plain language, it has been the practice of the United States Attorney's Office for the District of Columbia (and United States Attorney's Offices around the country) not to notify the subscriber or customer of an e-mail account that is the subject of an ECPA warrant.⁴

Requiring such notice would have a significant negative impact on how investigations are conducted in the District of Columbia. Perhaps unsurprisingly, the e-mail accounts for which disclosure is compelled pursuant to an ECPA warrant are commonly used by subjects or

⁴ Indeed, since Magistrate Judge Facciola issued his Memorandum Order on July 21, 2010, Magistrate Judge Kay has continued to give effect to the analysis of that Order, and in 14 other cases, of which we are aware, he has checked the box on the face of the ECPA warrants, requiring the Government, after a period of delay, to give notice to the subscriber or customer of the email account that was the subject of the ECPA warrant. See Case No. 10-423-M-01; Case No. 10-424-M-01; Case No. 10-425-M-01; Case No. 10-429-M-01; Case No. 10-430-M-01; Case No. 10-431-M-01; Case No. 10-432-M-01; Case No. 10-433-M-01; Case No. 10-434-M-01; Case No. 10-435-M-01; Case No. 10-436-M-01; Case No. 10-437-M-01; Case No. 10-438-M-01; and Case No. 10-442-M-01. Filed herewith is a Motion to Stay any notice obligation imposed in those cases, as well as this one, pending resolution of this Motion for Review by the Chief Judge of this Court.

As far as we have been able to determine, ECPA warrants presented to Magistrate Judge Deborah A. Robinson and to Chief Judge Royce C. Lamberth since July 21, 2010, did not have the delayed notification box checked. See Case No. 10-400-M-01; Case No. 10-408-M-01; and Case No. 10-456-M-01. We are unaware of any ECPA warrant presented to Magistrate Judge Facciola since July 21, 2010. We note, however, that during June 2010 Magistrate Judge Facciola signed five ECPA warrants without checking the delayed notification box. See Case No. 10-331-M-01; Case No. 10-347-M-01; Case No. 10-348-M-01; Case No. 10-349-M-01; and Case No. 10-350-M-01. Likewise, during June 2010 Magistrate Judge Robinson signed three ECPA warrants, and Chief Judge Lamberth signed one, without checking the delayed notification box. See Case No. 10-299-M-01; Case No. 10-300-M-01; Case No. 10-302-M-01; and Case No. 10-359-M-01.

UNDER SEAL

targets of the criminal investigation at issue, and the e-mail evidence derived from those compelled disclosures frequently forms the core of the Government's evidence supporting criminal charges. It is also sometimes the case during complex federal investigations spanning years that multiple ECPA warrants are sought and issued concerning the same e-mail account. Indeed, where there is no statute of limitations, some investigations are continued for many years because, while the evidence is not yet sufficient to bring charges, it is sufficient to have identified criminal subjects and/or criminal activity serious enough to justify continuation of the investigation. Thus, requiring the Government to provide prior notice to the subscriber or customer of an e-mail account before an ECPA warrant is issued, even if that notice could be subject to repeated requests for delay every 90 days while the investigation is ongoing, would pose a great burden both on the Government and this Court⁵ with little corresponding benefit to the privacy interest that the notice would purportedly seek to protect, as such repeated requests would routinely be granted if the e-mail account was used by a subject or target of an ongoing criminal investigation.

II. ARGUMENT

As demonstrated below, the Magistrate Judge's July 21, 2010 Memorandum Order should be reversed for three independent reasons. First, it is contrary to the plain language of ECPA's notice provisions and case law interpreting the Government's obligations under those provisions. Second, the Magistrate Judge erred in concluding that Fed. R. Crim. P. 41(f)(1)(C)'s

⁵ Magistrate Judge Facciola held that the Government's notice obligation with respect to an ECPA warrant could be delayed under 18 U.S.C. § 3103a. Mem. Order at 11. Section 3103a(d) requires that this Court report to the Administrative Office of the United States Court the fact of any warrant authorizing delayed notice under section 3103a, as well as any extension of that delayed notice, and the number and duration of any such extensions. 18 U.S.C. § 3103a(d).

UNDER SEAL

receipt provisions for Rule 41 warrants are incorporated into ECPA's provisions regarding warrants for the compelled disclosure of electronic communications. Third, even assuming that Rule 41(f)(1)(C)'s receipt provisions were incorporated into ECPA, they would be satisfied by providing notice to the third party, typically an Internet Service Provider ("ISP"), from whom the disclosure of the evidence at issue is compelled pursuant to an ECPA warrant.

A. Neither the Plain Language of ECPA's Notice Provisions, Nor Case Law Interpreting Those Provisions, Requires Notice to a Subscriber or Customer of an E-mail Account that is the Subject of an ECPA Warrant

The Magistrate Judge's conclusion that section 2703(b)(1)(A) of ECPA requires notice to the subscriber or customer of the e-mail account at issue (see Mem. Order at 8-9) is contrary to the plain language of the statute, as other courts have found. The starting point of statutory interpretation "is 'the language [of the statute] itself.'" Ardestani v. INS, 502 U.S. 129, 135 (1991), quoting United States v. James, 478 U.S. 597, 604 (1986). Section 2703(b)(1) states in pertinent part:

(1) A government entity may require a provider of remote computing service⁶ to

⁶ ECPA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). An "electronic communications system" is "any wire, radio, electromagnetic, photooptical or photoelectronic facilit[y] for the transmission of wire or electronic communications, and any computer facilit[y] or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14). A public ISP providing e-mail service to its customers, like Google here, is properly considered a provider of remote computing service with respect to opened e-mails maintained in the ISP's computer storage for the benefit of its customers. See Flagg v. City of Detroit, 252 F.R.D. 346, 362-63 (E.D. Mich. 2008). Such an ISP may also be considered a provider of "electronic communication service" within the meaning of ECPA with respect to the e-mail service that it provides to its employees. See 18 U.S.C. § 2711(1) (incorporating definitions of 18 U.S.C. § 2510) and 18 U.S.C. § 2510(15) (defining "electronic communication service" to mean "any service which provides users thereof the ability to send or receive wire or electronic communications"). See, e.g., Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114-15 (3rd Cir. 2004) (insurance company that

UNDER SEAL

disclose the contents of any wire or electronic communication . . . —

- (A) *without required notice to the subscriber or customer*, if the government entity obtains a *warrant* issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction; or
- (B) *with prior notice from the governmental entity to the subscriber or customer* if the government entity —
 - (i) uses an administrative *subpoena* authorized by a Federal or State statute or a Federal or State Grand jury or trial subpoena; or
 - (ii) obtains a *court order* for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

18 U.S.C. § 2703(b)(1) (emphasis added). Thus, the plain language of ECPA explicitly states that the Government need not give notice to the subscriber or customer of an e-mail account, where an ECPA warrant compels the disclosure of the contents of that account. See 18 U.S.C. §2703(b)(1)(A). Rather, such notice is required only if the Government seeks such content through a subpoena or section 2703(d) court order. See 18 U.S.C. §2703(b)(1)(B).

ECPA's delayed notice provision further confirms section 2703(b)(1)(A)'s already unambiguous language. K-Mart Corp v. Cartier, Inc., 486 U.S. 281, 291 (1988) (a particular phrase must be construed in light of the structure of the statute as a whole). It provides for delay of the notification required under section 2703(b) only with respect to "court orders" and "subpoenas" and makes no mention of warrants. See 18 U.S.C. § 2705(a). Plainly, had Congress intended to require notice to the subscriber with regard to the compelled disclosure of

provided e-mail service to its employees is a provider of electronic communication service within the meaning of ECPA).

UNDER SEAL

electronic communications through a warrant, it would have permitted delayed notification of the same sort available in connection with the use of a subpoena or court order. The fact that Congress did not do so in section 2705(a) demonstrates that Congress did not intend to impose such a notice obligation when disclosure of the e-mail contents was compelled by an ECPA warrant.

Similarly, the language of section 2703(c)(3) also confirms that Congress intended to allow ECPA warrants to be issued without notice to the subscriber or customer. Under section 2703(c)(1)(A), an ECPA warrant can be used to obtain all non-content records pertaining to a customer or subscriber. See 18 U.S.C. § 2703(c)(1)(A). In such cases, section 2703(c)(3) specifies that the Government “is not required to provide notice to a subscriber or customer.” Id. This provision further confirms the already unambiguous “without required notice” language in section 2703(b)(1)(A) and demonstrates that Congress understood that ECPA warrants would not require notice to the subscriber or customer. Thus, the Magistrate Judge erred when he “read into the language” of section 2703(b) “what is not there.” United States v. Murphy, 35 F.3d 143, 145 (4th Cir. 1994).

For similar reasons, the Magistrate Judge’s reliance on the delayed notification provisions in 18 U.S.C. § 3103a (Mem. Order at 7-8, 9-10) is misplaced. Preliminarily, section 3103a is not part of ECPA. Rather, Congress included its own specific delayed notification provision in the statute when it was enacted in 1986. See Pub. L. No. 99-508, § 201, 100 Stat. 1848 (1986) (including delayed notification provision of 18 U.S.C. § 2705). The delayed notification provision of section 3103a was enacted 15 years later as part of the USA PATRIOT Act of 2001. See Pub. L. No. 107-56, § 213, 115 Stat. 272, 286 (2001) (enacting delayed

UNDER SEAL

notification provision of 18 U.S.C. § 3103a(b)). There is no evidence that the USA PATRIOT Act amendment was directed in any way toward ECPA warrants or was designed to impose a new notice requirement on the Government. See id. Indeed, section 3103a, which is commonly referred to as the “sneak and peek” statute, makes no reference to compelled disclosures from providers of electronic communication services or remote computing services, the rules for which Congress meticulously delineated in ECPA. Compare 18 U.S.C. § 3103a with 18 U.S.C. §§ 2701-2710.⁷ Those specific ECPA provisions, which again make no mention of notice to the subscriber or customer of an e-mail account that is the subject of an ECPA warrant, trump the

⁷ To be sure, a subsection 3103a(b)(2) refers to “chapter 121,” which is ECPA, and to “wire and electronic communication” and “stored wire or electronic information” which are terms found in ECPA. See 18 U.S.C. § 3103a(b)(2). The mention of these terms in section 3103(b)(2) is unremarkable. That subsection generally prohibits the seizure of tangible and intangible property from a location to be searched pursuant to a “sneak and peek” warrant unless the Government demonstrates a “reasonable necessity for the seizure” of those items. See id. Specifically, a court must “prohibit the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure.” Id. Congress thus recognized that the Government may have a need to seize both tangible and intangible property even during a “sneak and peek” search, and section 3103a(b)(2) defines the legal standard for a court’s evaluation of such requests. Further, that subsection recognizes that certain intangible property, namely “stored wire and electronic information” (as opposed to a “wire and electronic communication”), is rightfully considered less sensitive even within ECPA (i.e., “except as expressly provided in Chapter 121”) and need not satisfy the “reasonable necessity” standard before it can be seized during a “sneak and peek” search. See 18 U.S.C. § 2703(c)(1) and (3) (ECPA provisions defining electronic information and indicating that such information can be acquired by the Government from third parties without notifying the subscriber or customer to whom the information relates). Further, the provision of ECPA that addresses the compelled disclosure of electronic information, i.e., section 2703(c), is separate and apart from the provisions of ECPA that compel the disclosure of the contents of an e-mail account. Compare 18 U.S.C. § 2703(a) and (b)(1)(A); with 18 U.S.C. § 2703(c). Conflating these provisions, the Magistrate Judge erroneously concluded that “Congress had to have understood that [ECPA] and § 3103a would be read together to permit delay of notification of warrants issued under [ECPA] and Rule 41,” and specifically to ECPA warrants compelling the disclosure of the contents of an e-mail account under section 2703(a) and (b)(1)(A).

UNDER SEAL

more general provisions of section 3103a located outside of ECPA. In any event, section 3103a (like section 2705(a)) does not itself impose a notice requirement. Rather, by its own language, it simply provides a procedure to delay “any notice required, or that may be required.” 18 U.S.C. § 3103a(b). Because no notice of an ECPA warrant is required under section 2703(b)(1)(A) to the subscriber or customer whose e-mail account is the subject of the ECPA warrant, the delayed notification provisions of section 3103a, by its own terms, are inapplicable.

This plain language interpretation of section 2703(b)(1)(A) is also consistent with the case law. See Guest v. Leis, 255 F.3d 325, 338-39 n. 7 (6th Cir. 2001) (finding “[un]supported by the statute” an interpretation of ECPA requiring notice to subscribers when the Government compels disclosure pursuant to an ECPA warrant). As the court held in Bansal v. Russ, 513 F. Supp. 2d 264, 276-77 (E.D. Pa. 2007), the Government “need not provide notice of . . . search warrants to [a subscriber or customer of an e-mail account] under [ECPA]; it is only if the government elects to obtain the information via subpoena that it must provide notice to the subscriber or customer.” See also United States v. Weiner, 2:09CR87-NBB-DAS, 2009 WL 2923068, *1 (N.D. Miss. 2009) (unpublished). But see Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993) (assuming, without statutory analysis, that ECPA’s notice provisions are applicable to a warrant), aff’d on different issue by, 36 F.3d 457 (5th Cir. 1994).

Nor does this plain language interpretation of section 2703(b)(1)(A) lead to an “irrational” result as suggested by the Magistrate Judge. See Mem. Order at 10-11. Indeed, it makes sense that Congress fashioned ECPA’s notice obligations to distinguish between circumstances where the Government compels third-party disclosure of e-mail content based on

UNDER SEAL

a warrant that is supported by probable cause and subject to judicial supervision, and those where the Government issues a subpoena or obtains a court order under section 2703(d) based on the lower standard of reasonable suspicion.⁸ Where the process requires less scrutiny and proof than a warrant, Congress created a statutory right to notice that is otherwise not required. This interpretation of the statute is also consistent with other areas of federal criminal procedure which seek to balance an individual's privacy interests with the Government's compelling interest in enforcing the criminal law. In fact, Congress has long-since established a number of means by which the Government can use third-party process to further a criminal investigation without notice to the target of the investigation, including the use of certain search warrants, grand jury subpoenas, and pen register orders. Indeed, the Supreme Court has held that there is no basis – constitutional or otherwise – for requiring that the target of an investigation receive notice of a subpoena directed at third parties. See SEC v. O'Brien, 467 U.S. 735, 742-43 (1984). There is even less reason to impose such a notice requirement on the issuance of a warrant which, unlike a subpoena, requires a showing of probable cause and is subject to authorization and supervision by a neutral, detached magistrate judge.

B. Fed. R. Crim. P. 41(f)(1)(C)'s Receipt Provisions are Inapplicable to Warrants Issued under ECPA

The Magistrate Judge erred in assuming that Fed. R. Crim. P. 41(f)'s provisions

⁸ Specifically, issuance of a section 2703(d) order does not require probable cause but only “specific and articulable facts showing that there are reasonable grounds to believe that the contents of the wire or electronic communication . . . are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). The legislative history of ECPA makes clear that the “specific and articulable facts” standard is “an intermediate standard . . . higher than a subpoena, but not a probable cause warrant.” H. Rep. No. 827, 103d Cong., 2d Sess. 31 (1994) (emphasis added), reprinted in 1994 U.S. Code Cong. & Admin News 3489, 3511.

UNDER SEAL

regarding the execution and return of a search warrant are incorporated into section 2703(b)(1)(A) of ECPA by virtue of the latter's statutory provision that a warrant thereunder must be "issued using the procedures described in the Federal Rules of Criminal Procedure." 18 U.S.C. § 2703(b)(1)(A) (emphasis added). See Mem. Order at 7 (assuming, without discussion, that Fed. R. Crim. P. 41(f)(1)(C)'s receipt provisions required notice to the subscriber or customer whose account is the subject of a warrant issued under ECPA). Preliminarily, a warrant issued under ECPA is not a Rule 41 search warrant. If there had been any doubt about this before, Congress eliminated it when Congress amended the relevant language of ECPA as part of the USA PATRIOT Act of 2001, striking the language "a warrant issued under the Federal Rules of Criminal Procedure" everywhere it appeared in ECPA and replacing that language with "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure." See Pub. L. No. 107-56, § 220(a)(1). Furthermore, unlike a Rule 41 search warrant, which authorizes law enforcement officers to search and seize persons or property, see Fed. R. Crim. P. 41(c), an ECPA warrant calls for the compelled disclosure of the contents of wire or electronic communications or other records and information outside the presence of law enforcement officers. See 18 U.S.C. § 2703.

Contrary to the Magistrate Judge's unsupported assumption that notice to the subscriber or customer is required, by its plain language section 2703(b)(1)(A) of ECPA incorporates only those procedural provisions of Rule 41 that relate to the issuance of the warrant (i.e., Rule 41(d) and (e)), and not to the provisions of Rule 41 that relate to the execution and return of the warrant (i.e., the entirety of Rule 41(f)). See 18 U.S.C. § 2703(b)(1)(A) (merely directing that a warrant thereunder be "issued using the procedures described in the Federal Rules of Criminal

UNDER SEAL

Procedure”) (emphasis added). Because Rule 41(f)(1)(C)’s receipt requirement concerns the execution and return of a search warrant, it does not apply to the issuance of a warrant under ECPA. Further, it would be incongruous to apply Rule 41(f)’s execution and return provisions to ECPA warrants. This is particularly so, where Rule 41(f) describes steps a law enforcement officer must take while present for the execution of the search warrant, such as noting the time of execution, inventorying the property seized, and providing a copy of the warrant and a receipt. See Fed. R. Crim. P. 41(f)(1)(A)-(C). By contrast, ECPA specifically provides that the presence of a law enforcement officer “shall not be required for service or execution” of an ECPA warrant. See 18 U.S.C. § 2703(g). Indeed, quite unlike Rule 41(f)’s requirements and in reliance on section 2703(g), law enforcement officers frequently serve ECPA warrants on ISPs by facsimile.⁹

The Seventh Circuit recently reviewed this language in ECPA – albeit under section 2703(a), not section 2703(b)(1)(A)¹⁰ – and concluded that the statute “refers only to the specific

⁹ Furthermore, Rule 41 itself provides that it “does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances.” Fed. R. Crim. P. 41(a). Congress created such a “special circumstance” with Section 2703(a). See United States v. Berkos, 543 F.3d 392, 398 & n. 6 (7th Cir. 2008); In the Matter of the Search of Yahoo, Inc., No. 07-3194-MB, 2007 WL 1539971 at *7 (D. Ariz. May 21, 2007) (unpublished); In re Search Warrant, No. 6:05-MC-168-Orl-31JGG, 2005 WL 3844032 at *6 n. 16 (M.D. Fla. Feb. 13, 2006) (unpublished).

¹⁰ The distinction between these two subsections is immaterial to the issue at hand. Section 2703(a) concerns compelled disclosure from a provider of electronic communications service, while section 2703(b)(1)(A) concerns compelled disclosure from a provider of remote computing service. Each type of service is separately defined by statute. See 18 U.S.C. §§ 2711(1) and 2510(15) (electronic communication service); 18 U.S.C. § 2711(2) (remote computing service). See footnote 6 above. Further, both subsections include the same statutory language, discussed above, directing that warrants under either provision be “issued using the procedures described in the Federal Rules of Criminal Procedure.” See 18 U.S.C. § 2703(a) and 2703(b)(1)(A) (emphasis added). The interpretation of those two identical provisions should be

UNDER SEAL

provision of the Rules of Criminal Procedure, namely, Rule 41, that detail the procedures for obtaining and issuing warrants.” United States v. Berkos, 543 F.3d 392, 398 (7th Cir. 2008) (emphasis in original). Other courts to consider the issue have reached the same conclusion. See, e.g., In re Search of Yahoo, Inc., No. 07-3194-MB, 2007 WL 1539971 at *6 (D. Ariz. May 21, 2007) (unpublished); In re Search Warrant, No. 6:05-MC-168-Orl-31JGG, 2005 WL 3844032 at *5-*6 (M.D. Fla. Feb. 13, 2006) (unpublished); and United States v. Kernell, No. 3:08-CR-142, 2010 WL 1408437, *4 (E.D. Tenn. 2010) (unpublished). While one district court reached the opposite conclusion about the applicability of Rule 41(f) to an ECPA warrant, that court nevertheless held that any notice requirement was met by serving the ECPA warrant on the third-party ISP, an issue we address in the following section. See In the Matter of the Application of the United States of America for a Search Warrant, 665 F. Supp. 2d 1210 (D. Or. 2009).¹¹

the same; because section 2703(b)(1)(A) plainly does not require notice for a warrant issued thereunder, neither should section 2703(a). Indeed, the explicit language in section 2703(b)(1)(B) requiring notice to subscribers or customers of subpoenas or section 2703(d) court orders for the content of electronic communications, demonstrates that when Congress wanted to require notice within ECPA it did so explicitly. Thus, it must be “presumed that Congress acted intentionally and purposely in the disparate . . . exclusion” of any such notice language in section 2703(a) – the section immediately prior to section 2703(b)(1)(A). Brown v. Gardner, 513 U.S. 115, 120 (1994).

¹¹ This prevailing interpretation of ECPA is also consistent with the legislative history of the 2001 amendments of ECPA, which were part of the USA PATRIOT Act and “broaden[ed] the government’s ability to obtain warrants for electronic communications.” Berkos, 543 F.3d at 397 n. 4; see also Kernell, 2010 WL 1408437, *4. Given this – as well as the legal presumption that Congress intended to change the meaning of the statute when it changed the language of it – the Magistrate Judge erred in relying on the legislative history from the 1986 version of ECPA. See Mem. Order at 9, 11.

UNDER SEAL

C. Fed. R. Crim. P. 41(f)(1)(C)'s Receipt Provisions are Satisfied in the Third-Party Context by Serving the Warrant on the Holder of the Property

The Magistrate Judge further erred in assuming that in the third-party context law enforcement officers are required to serve a copy of a search warrant on both the holder of the property and the owner of the property. To the contrary, assuming arguendo that Fed. R. Crim. P. 41(f)(1)(C)'s receipt provisions applied to ECPA warrants – which, we have shown, they do not – that rule would be satisfied by serving the warrant on the ISP. There is no requirement in Rule 41 to provide “notice” to a property owner that a third party’s premises have been searched and the owner’s property has been seized. Therefore, there would be no requirement, even under the Magistrate Judge’s erroneous incorporation of Rule 41(f)(1)(C) into ECPA, to serve a copy of the ECPA warrant on the subscriber or customer of the e-mail account that was the subject of the warrant.

Although the Magistrate Judge referred in his Memorandum Order to “the notice thus required by Rule 41” (Mem. Order at 7), Rule 41 does not contain the word “notice.” Nor does the Rule require any such notice as contemplated by the Magistrate Judge. Instead, Rule 41(f)(1)(C) requires that:

The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property.

Again, the Magistrate Judge ignored the plain language of the provisions that he invoked to reach his decision.

In United States v. Zacher, 465 F.3d 336, 339 (8th Cir. 2006), in an opinion authored by Judge Arnold, the Eighth Circuit rejected the defendant’s argument that the police violated a

UNDER SEAL

state rule of criminal procedure virtually identical to Rule 41(f), by failing to provide him with a copy of a search warrant and receipt for property seized from a FedEx facility. The Eighth Circuit held that the police complied with the rule by leaving a copy of the warrant at the FedEx facility. Id. Moreover, the Eighth Circuit held that it was “immaterial” that the defendant was not notified of the search. Id.

Analogizing to Zacher, in In the Matter of the Application of the United States of America for a Search Warrant, the district court found that Rule 41(f)(1)(C)’s receipt provisions were satisfied without notice to the e-mail account holder:

In this case, the warrant was served on Google and Webhost for electronic information stored on the companies’ servers. The ISPs are analogous to FedEx in Zacher; the electronic information was stored on the servers at Google and Webhost the same way the package was stored at FedEx. Requiring notice to the subscriber ignores this third-party context. When the property to be seized is in the possession of a third party, Rule 41(f)(1)(C) requires no more than what was already accomplished in this case.

665 F. Supp. 2d at 1221-22. In its ruling, the district court also observed that “[t]he word ‘notice’ is never used” in Rule 41. Id. at 1221. Therefore, without conceding that Rule 41(f) even applies to an ECPA warrant, that Rule would not require notice to the e-mail account holder in this case, because the evidence disclosed pursuant to the ECPA warrant was obtained from a third party, namely Google. Thus, service of the ECPA warrant on Google would be sufficient under Rule 41.

UNDER SEAL

III. CONCLUSION

Wherefore, the Government respectfully requests that the Court reverse the Magistrate Judge's July 21, 2010 Memorandum Order and hold that the Government has no obligation to provide notice to the subscriber or customer of an e-mail account that is the subject of a warrant issued under ECPA.

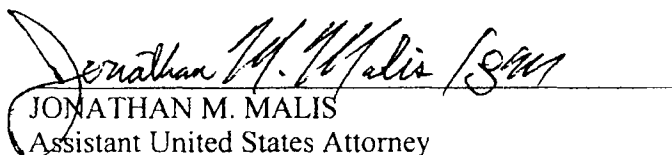
Respectfully submitted,

RONALD C. MACHEN JR.
UNITED STATES ATTORNEY
D.C. Bar Number 447-889

By:



G. MICHAEL HARVEY
Assistant United States Attorney
D.C. Bar Number 447-465
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-439
Washington, D.C. 20530
Phone: (202) 305-4155
Michael.Harvey2@usdoj.gov



JONATHAN M. MALIS
Assistant United States Attorney
D.C. Bar Number 454-548
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-447
Washington, D.C. 20530
Phone: (202) 305-9665
Jonathan.M.Malis@usdoj.gov

Dated: September 3, 2010

Exhibit A

FILED

SEP - 3 2010

Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

07/21/2010 16:31 FAX 202 354 30
USDC CRIMINAL DIVISION

USDC CRIMINAL DIVISION

002/014

<https://ecf.dcd.circdc.dcn/cgi-bin/Dispatch.pl?129154992837665>

Other Orders/Judgments

1:10-mj-00291-AK *SEALED* USA v. E-MAIL ACCOUNT

[REDACTED]@GMAIL.COM ON COMPUTER SERVERS OPERATED BY
GOOGLE, INC., 1600 AMPHITHEATRE PARKWAY, MOUNTAIN VIEW, CALIFORNIA
CLOSED, Sealed_Case

U.S. District Court

District of Columbia

Notice of Electronic Filing

The following transaction was entered on 7/21/2010 at 2:55 PM and filed on 7/21/2010

USA v. E-MAIL ACCOUNT [REDACTED]@GMAIL.COM ON COMPUTER
Case Name: SERVERS OPERATED BY GOOGLE, INC., 1600 AMPHITHEATRE PARKWAY,
MOUNTAIN VIEW, CALIFORNIA

Case
Number: 1:10-mj-00291-AK *SEALED*

Filer:

Document
Number: No document attached

Docket Text:

MINUTE ORDER as to E-MAIL ACCOUNT [REDACTED]@GMAIL.COM ON
COMPUTER SERVERS OPERATED BY GOOGLE, INC., 1600 AMPHITHEATRE PARKWAY,
MOUNTAIN VIEW, CALIFORNIA: MINUTE ORDER: I have issued a Memorandum Order
regarding the government's motion for clarification. I have filed the Memorandum Order
under seal; however, the Order to Seal issued in this case by Magistrate Judge Kay
does not extend to my Memorandum Order. Thus, the government is hereby ORDERED
to show cause in writing within five days of this order why I should not unseal the
Memorandum Order for public view. The unsealed version of the Memorandum Order
would be subject to the redaction of the e-mail address at issue in the case and any
language that would identify the e-mail address or topic of the investigation. SO
ORDERED. Signed by Magistrate Judge John M. Facciola on 07/21/10. (zldc,)

1:10-mj-00291-AK *SEALED*-1 No electronic public notice will be sent because the case/entry is
sealed.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT
FOR E-MAIL ACCOUNT

██████████@GMAIL.COM
MAINTAINED BY GOOGLE, INC.,
HEADQUARTERED AT 1600
AMPHITHEATRE PARKWAY,
SUNNYVALE, CA

Mag. No. 10-mj-291 (AK/JMF)
(Under seal)

MEMORANDUM ORDER

The government has filed a Motion for Clarification of Notice Obligations of E-mail Search Warrant ("Mot."), seeking clarification of the Court's decision to check the box on the face of the warrant finding that immediate notification of the warrant "to the person who, or whose property, will be searched or seized" would "have an adverse result listed in 18 U.S.C. § 2705" and permitting delayed notification for up to 30 days. See Mot. at Ex. 2, Search and Seizure Warrant ("Warrant").

I. Introduction

In an opinion I wrote several years ago, I questioned whether a person's location as detected by the use of geolocation information created by her cell phone could ever constitute evidence subject to seizure under Rule 41 of the Federal Rules of Criminal Procedure.¹ Then-Chief Judge Hogan reviewed the denial of an application for such a

¹ In that opinion, I indicated that "if the government's quoted statement is an invocation of the Fourth Amendment standard, it fails to capture the entire force of that Amendment—that it permits the issuance of a warrant upon a showing that there is probable cause to believe that whatever is to be seized is '(1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime.' Fed. R. Crim. P. 41(c); Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 308 (1967). Putting aside the complicated question of whether a person's location could in itself meet any of these criteria, it is

warrant by another magistrate judge in the Court and determined that a person's location could be evidence of a crime. See In re U.S. for an Order Authorizing Monitoring of Geolocation and Cell Site Data for a Sprint Spectrum Cell Phone Number, Nos. 06-mc-186, 187, and 188, 2006 WL 6217584, at *4 n.6 (D.D.C. Aug. 25, 2006) (finding that "[c]ell site and geolocation information may be evidence of a crime because, for example, a subject's location can be used to rebut an alibi or place him at the scene of a crime"). Ever since that decision, the United States Attorney's Office for the District of Columbia (USAO), while protecting its objection that it is not required to show probable cause in each application, has consistently made a showing of probable cause when seeking prospective geolocation data.

In seeking geolocation data, the government typically also invokes 18 U.S.C. § 3103a(b),² which allows any required notice of the warrant to be delayed in certain circumstances. See 18 U.S.C. § 3103a(b). When granting such a delay under this statute, the Court is required to report the approval of such a delay to the Administrative Office of the United States Courts ("AO"). See 18 U.S.C. § 3103a(d). The AO revised its search warrant form, recommended for use by the federal courts, to include a box that the issuing judge must check to indicate that she has found reasonable cause to approve a delay in notifying the party subject to the search of the existence of a warrant. See AO

certainly clear that probable cause to believe that a person's location is relevant to a criminal investigation cannot possibly meet the constitutional standard the government purports to invoke, that it is more likely than not that what is [to] be seized is evidence, contraband, fruits of a crime or designed to be used to commit a crime." In re Application of U.S. for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 132, 133 (D.D.C. 2005).

² All references to the United States Code are to the electronic version in Westlaw or Lexis.

93 (Rev. 12/09) Search and Seizure Warrant. The judge then specifies on the warrant the number of days such notice may be delayed. Id. This is done pursuant to the statutory authority granted by 18 U.S.C. § 3130a(b) that permits such delay in notification; but for that statute, the executing officer would have to give the party subject to the search a copy of the warrant and a receipt for what the officer has taken. Fed. R. Crim. P. 41(f)(1)(C). Thus, the government, using this form, may seek to delay notification by having the judge check the box, but it may not completely abdicate its responsibility under Rule 41(f)(1)(C); eventually, the cell phone subscriber whose whereabouts are being tracked will ultimately receive a copy of the warrant, which authorized the government to gather the geolocation data from the phone without her knowledge.

In this case, the government is not seeking geolocation data from a cell phone. Instead, the government seeks to search the contents of a person's e-mail account, pursuant to the Stored Communications Act ("SCA"). See Warrant. I only recount the history of geolocation warrants because it highlights an incongruity in the government's position. In this case, the government objects to having to provide any notice to the subscriber of the account being searched. Mot. at 1. According to the government, notice to the e-mail account provider is sufficient. The subscriber therefore will never know, by being provided a copy of the warrant, for example, that the government secured a warrant and searched the contents of her e-mail account. In comparison, the user of a cell phone whose telecommunications data has been intercepted and captured pursuant to a warrant would ultimately learn that the government has been surveilling her, even though a portion of that surveillance may have occurred when she was in a public place. The e-mail account holder, on the other hand, would never learn of the search of the entire

contents of her e-mail account. Thus, as the government would have it, while it would have to tell a person that it followed his movements one day as he walked from K Street to Connecticut Avenue, it would never have to tell him that it has read and copied the entire contents of the e-mail account that he opened when he arrived at his office on K Street.

The incongruity of that position compels me to conclude that the more appropriate interpretation of the pertinent portions of the SCA and of Rule 41 of the Federal Rules of Criminal Procedure is that Congress intended that the person whose e-mail account is seized by the government ultimately receives notice of that seizure, even though that notification may be delayed, if the requirements of the applicable statutes are met.

II. Background

On May 28, 2010, USAO sought a search warrant for a particular Google E-mail ("Gmail") account. Mot. at 1. The Court, per Magistrate Judge Kay, granted the request, and, when signing the warrant, checked the box on the AO 93 (Rev. 12/09) Search and Seizure Warrant, which indicated that the Court found that "immediate notification of the warrant 'to the person who, or whose property, will be searched or seized' would 'have an adverse result listed in 18 U.S.C. § 2705' and permitted delayed notification for up to 30 days." Mot. at 1 (citing AO 93 (Rev. 12/09) Search and Seizure Warrant). In its application for the search warrant, the government, however, did *not* seek delayed notification. See Mot. at Ex. 1, Application for Search Warrant. Yet, my colleague, Magistrate Judge Kay, checked the box granting delayed notification. The government now seeks to be excused from its obligations to provide notice, because it does not

believe there to be any such notice obligation for e-mail search warrants under 18 U.S.C. § 2703(b)(1)(A). Mot. at 1.

The government is incorrect in its assumption; notice of a search warrant is required, even if the warrant was issued under 18 U.S.C. § 2703(b)(1)(A). Any other interpretation of the statute would lead to the insupportable conclusion that Congress intended the government to copy and read the entirety of the e-mail messages, and yet to never be required to provide notice to the owner of the e-mail account.

III. Analysis

The SCA has proven to be enormously difficult to understand and apply, probably because the technology has advanced so rapidly since its enactment in 1986. See 18 U.S.C. § 2701 *et seq.* The SCA protects e-mail subscribers from unlawful access or involuntary disclosure of their stored communications or records,³ but also provides for the compelled disclosure of customer communications or records. 18 U.S.C. § 2703. Under § 2703, the government can require a provider to disclose the contents of wire or electronic communications. Id. There is an anachronistic curiosity within the SCA; the governmental entity seeking the disclosure must follow different procedures based on whether the communication sought is a wire or electronic communication in “electronic storage”⁴ or in a “remote computing service.”⁵

³ 18 U.S.C. §§ 2701-02.

⁴ The definition of electronic storage is: “(1) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (2) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17)(A)-(B).

⁵ “Remote computing service” refers to “the provision to the public of computer storage or processing services by means of an electronic communications system.” 18 U.S.C. § 2711(2).

While the SCA provides definitions of these terms, they were developed before the advent of prolific and free cloud computing, where a user can sign up for a free e-mail account with a subscriber and have essentially unlimited storage for e-mails. The amount of information stored in modern American business or personal e-mail accounts can be staggering. E-mail providers compete against each other by offering storage space for free. Apple's e-mail accounts, for example, come with 20 gigabytes of free storage.⁶ Microsoft offers 10 free gigabytes of storage to student users of Outlook.⁷ Google continually adds available storage space, even as one is logging into one of its accounts.⁸ With such storage capacity, the user can be expected to store thousands of sent and received messages, even those the user has designated to be "trash."

The contents of these stored e-mails are as varied as the users, but it is surely reasonable to expect that e-mail accounts contain banking, tax, and other financial information as well as more personal and intimate communications.

With its warrant, the government seeks the contents of a Gmail account under §2703(b)(1)(A), which refers to contents in a remote computing service and reads:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection -

⁶ See Apple MobileMe Home Page, <http://www.apple.com/mobileme/pricing/> (last visited Jul. 20, 2010).

⁷ See Microsoft Live@Edu Home Page, <http://www.microsoft.com/liveedu/free-hosted-student-email.aspx> (last visited Jul. 20, 2010).

⁸ See Gmail by Google Home Page, <http://mail.google.com/mail> (last visited Jul. 20, 2010).

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity –

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

18 U.S.C. § 2703(b).

The government may therefore, without notice to the subscriber, invoking the powers and limitations of Rule 41 of the Federal Rules of Criminal Procedure; one limitation of the rule is, of course, the obligation to give a copy of the warrant and a receipt for the property taken "to the person from whom . . . the property was taken." Fed. R. Crim. P. 41(f)(1)(C).

While not part of the SCA, a separate statute permits the notice thus required by Rule 41 to be delayed. 18 U.S.C. § 3103a(b). Therefore, as the government has done in its applications for warrants seeking geolocation data, and as the form permits, notification of the existence of a search warrant for an e-mail account can be delayed; however, it must ultimately be given. Under the SCA,

given to the subscriber of an e-mail account if the government seeks a

warrant under 18 U.S.C. §2703(b)(1)(A). The procedural terms of Rule 41, however, incorporated into the SCA, require that a copy of the warrant be given "to the person from whom . . . the property was taken." Fed. R. Crim. P. 41(f)(1)(C). Notice, however, may be delayed according to 18 U.S.C. § 3103a(b).

The complication comes about when one realizes that the SCA contains its own authority for delaying notice of an order that the SCA itself authorizes. If probable cause to search an e-mail account is not available, the government may still get a court order requiring disclosure of the account, if the government nevertheless asserts "specific and articulable facts" showing reasonable grounds to believe that the contents of the account "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Once again, however, Congress requires that notice be ultimately given to a subscriber, but permits a delay in the required notice to the subscriber (as articulated in 18 U.S.C. § 2703(e)(1)(B)) if certain requirements (not pertinent here) are met. See 18 U.S.C. § 2705.

Read together, whether the government proceeds by seeking a search warrant, premised on probable cause, or by seeking a court order, premised on "specific and articulable facts," notice must be given to the subscriber, but it may be delayed.

The only other way to read the pertinent provision of the SCA that provides that the government may secure a search warrant "without required notice" to the subscriber is to read it to dispense with the government's ever being obliged to give notice to the subscriber. But, the subsection that seems to dispense with notice simultaneously requires that the government use the procedures in the Federal Rules of Criminal Procedure and one of those procedures is, unquestionably, the giving of notice, *i.e.*, the

leaving of a copy of the warrant and the receipt for what was taken. The plain text of the SCA therefore requires the very notice that the government seeks to avoid.

Further, the legislative history of the SCA indicates clearly that the purpose of the act was to address the expansion of opportunities for government intrusions created by the development of new methods of communication and devices for surveillance. S. Rep. No. 99-541, at 2 (1986). Accordingly, Congress asserted that "the law must advance with the technology to ensure the continued vitality of the fourth amendment . . . Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right." *Id.* at 5.

As such, note how carefully Congress has postponed the giving of notice of the disclosure of the contents of stored communications in the SCA itself and in 18 U.S.C. § 3103a. In § 3103a, a judicial officer may provide for delayed notice accordingly:

(b) Delay.— With respect to the issuance of any warrant under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if —

(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial);

(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and

(3) the warrant provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay.

18 U.S.C. § 3103a. The text of subsection (b)(2) specifically refers to the SCA, which is "chapter 121," and to stored wire and electronic communications. The SCA already provides for delayed notification of court orders and administrative subpoenas issued under § 2703(b) of the SCA. Thus, Congress had to have understood that the SCA and § 3103a would be read together to permit delay of notification of warrants issued under the SCA and Rule 41 of the Federal Rules of Criminal Procedure. Further, it only makes sense for Congress to have allowed for the delay of notification because it understood that notice was required to be given in the first place.

It can be said with confidence that Congress has never indicated that it considers the giving of notice as a mere formality. To the contrary, in this new world where the government can detect a person's location by her cell phone signals and read her e-mails, Congress has required notice but permitted its postponement. Indeed, even a warrant for a tracking device must ultimately be given to the person who has been tracked. It is irrational to think that Congress would, in the teeth of that care, grant the government a perpetual dispensation from ever notifying a person of the remarkable intrusion that a search of his e-mail account creates. In fact, in discussing the amendments made to 18 U.S.C. § 3103a, the legislative history makes clear that changes were made to ensure that, when utilizing the so-called "sneak-and-peek" warrant under 18 U.S.C. § 3103a, the government was prohibited from seizing any wire or electronic communication, or any stored electronic information, without a showing of reasonable necessity, *and* that notice

of the search of the same be given within a reasonable time of the execution of the warrant. See, e.g., 147 Cong. Rec. S11,002 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

Finally, the government's claim that notice to the Internet Service Provider ("ISP") complies with the notice requirement is unpersuasive. Why does an ISP need notice, via a copy of the warrant, when it is being served with the warrant or order? It is inconceivable that Congress, which took such care in identifying when and how notice to the person whose privacy has been invaded is to be given, would dispense with those requirements because of the meaningless act of telling the ISP what it already knows. The legislative history of the SCA tells us that Congress was concerned with "protect[ing] the sanctity and privacy of the communication" and "afford[ing] protection against governmental snooping in these files." 132 Cong. Rec. 14,886 (1986) (statement of Rep. Kastenmeier). One such protection provided by Congress in the SCA and Rule 41 of the Federal Rules of Criminal Procedure is notice.

Thus, for the reasons stated herein, it is, hereby,

ORDERED that the government's motion for clarification is **GRANTED**. It is further, hereby,

ORDERED that this Memorandum Order shall serve as the clarification the government seeks and shall confirm that the government is required to provide notice to the subscriber of the e-mail being searched, pursuant to Rule 41(f)(1)(C). Such notice may be delayed, as Magistrate Judge Kay has provided, according to 18 U.S.C. § 3103a(b), and that period of delay may be extended upon motion to the Court for such

extension. Nevertheless, eventually, the subscriber of the e-mail account to be searched shall receive a copy of the warrant as notice, pursuant to Rule 41(f)(1)(C).

SO ORDERED.



Digitally signed by
John M. Facciola
Date: 2010.07.21
14:14:32 -04'00'

JOHN M. FACCIOLA
UNITED STATES MAGISTRATE JUDGE

Exhibit B

MIME-Version:1.0

From:DCD_ECFNotice@dcd.uscourts.gov

To:DCD_ECFNotice@localhost.localdomain

Bcc:

--Case Participants:

--Non Case Participants:

--No Notice Sent:

Message-Id:<2652348@dcd.uscourts.gov>

Subject:Activity in Case 1:10-mj-00291-AK *SEALED* USA v. E-MAIL ACCOUNT

[REDACTED]@GMAIL.COM ON COMPUTER SERVERS OPERATED BY GOOGLE, INC.,
1600 AMPHITHEATRE PARKWAY, MOUNTAIN VIEW, CALIFORNIA Order on Motion to Vacate
Content-Type: text/html

This is an automatic e-mail message generated by the CM/ECF system. Please DO NOT RESPOND to this e-mail because the mail box is unattended.

*****NOTE TO PUBLIC ACCESS USERS***** Judicial Conference of the United States policy permits attorneys of record and parties in a case (including pro se litigants) to receive one free electronic copy of all documents filed electronically, if receipt is required by law or directed by the filer. PACER access fees apply to all other users. To avoid later charges, download a copy of each document during this first viewing. However, if the referenced document is a transcript, the free copy and 30 page limit do not apply.

NOTE: This docket entry (or case) is SEALED. Do not allow it to be seen by unauthorized persons.

U.S. District Court

District of Columbia

Notice of Electronic Filing

The following transaction was entered on 8/23/2010 at 6:01 PM and filed on 8/23/2010

USA v. E-MAIL ACCOUNT [REDACTED]@GMAIL.COM ON COMPUTER
Case Name: SERVERS OPERATED BY GOOGLE, INC., 1600 AMPHITHEATRE PARKWAY,
MOUNTAIN VIEW, CALIFORNIA

Case Number: 1:10-mj-00291-AK *SEALED*

Filer:

Document Number: No document attached

Docket Text:

MINUTE ORDER denying [7] Motion to Vacate: Having consulted with Magistrate Judge Kay on his decision to check the box delaying notification, I understand now that he believed the Government would still provide notice to the subscriber, regardless of whether it was delayed. In fact, upon the request of an Assistant United States Attorney, he withdrew the delayed notice; however, he believed the result in doing so would be that

the Government would notify the subscriber without any delay. Thus, he agrees with the analysis in my memorandum order and has authorized me to so state. Accordingly, seeing no grounds on which to vacate my order, it is hereby ORDERED that the motion to vacate is DENIED. It is further hereby ORDERED that the Government's motion to stay the unsealing of the memorandum order pending resolution of any appeal of that order to the Chief Judge is GRANTED. SO ORDERED. Signed by Magistrate Judge John M. Facciola on 08/23/2010. (lcjmf1)

1:10-mj-00291-AK *SEALED*-1 No electronic public notice will be sent because the case/entry is sealed.

EXHIBIT M

Chief of Staff, 1st Air Force
 1000 1st St. S.E. Columbus, GA

UNDER SEAL

On May 28, 2010, the Government applied to Magistrate Judge Alan Kay for a warrant pursuant to ECPA in Case No. 10-291-M-01. In issuing the warrant, Magistrate Judge Kay checked the box on the face of the new search warrant form issued this year by the Administrative Office of the United States Courts allowing for a 30-day delay of notification under 18 U.S.C. § 3103a, which delay had not been requested by the Government's application

UNDER SEAL

for the ECPA warrant. As a result, the Government was effectively ordered to make such notification – that is to notify the subscriber or customer of the e-mail account that was the subject of the ECPA warrant – no later than June 27, 2010. Meanwhile, on June 8, 2010, the Government filed a Motion for Clarification that sought to clarify Magistrate Judge Kay’s intent in checking the box.

Thereafter, on July 21, 2010, Magistrate Judge John M. Facciola (who, in July 2010, was the Magistrate Judge assigned to handle search warrant and related matters) issued a Memorandum Order in response to the Government’s Motion for Clarification. The Government thereafter filed a Motion to Vacate the Memorandum Order, which Magistrate Facciola denied by Minute Order, which was served on the Government on August 23, 2010. On September 2, 2010, the Government filed with the Chief Judge of this Court a Motion for Review of Magistrate Judge’s July 21, 2010, Memorandum Order regarding Notice Obligations for E-mail Warrants Issued Under ECPA (“Motion for Review”). As set forth in detail in the Motion for Review, the Government submits that the analysis in the Memorandum Order is incorrect, and that the Government has no obligation to provide notice to the subscriber or customer of an e-mail account that is the subject of a warrant issued under ECPA.

II. NEED FOR STAY OF NOTIFICATION ORDERS

As noted above, the ECPA warrant that is the subject of the Government’s Motion for Review required notification to the subscriber or customer of that e-mail account after a delay of 30 days, that is, until June 27, 2010. As this matter remains the subject of litigation, such notification has not yet been made.

UNDER SEAL

In addition, following the issuance of Magistrate Judge Facciola's Memorandum Order on July 21, 2010, Magistrate Judge Kay – serving as the Magistrate Judge assigned to consider applications for search warrants and related matters for the month of August 2010 -- continued to give effect to the analysis of the Memorandum Order. As far as we have been able to determine, fourteen ECPA warrants were presented to Magistrate Judge Kay and in all such cases he checked the box on the face of the ECPA warrant, requiring the Government, after a period of delay, to give notice to the subscriber or customer of the e-mail account that was the subject of the ECPA warrant. See Case No. 10-423-M-01; Case No. 10-424-M-01; Case No. 10-425-M-01; Case No. 10-429-M-01; Case No. 10-430-M-01; Case No. 10-431-M-01; Case No. 10-432-M-01; Case No. 10-433-M-01; Case No. 10-434-M-01; Case No. 10-435-M-01; Case No. 10-436-M-01; Case No. 10-437-M-01; Case No. 10-438-M-01; and Case No. 10-442-M-01.¹ Upon notification by Magistrate Judge Kay that he would require notification, the applicants for eleven of these ECPA warrants requested, and obtained, delayed notification periods longer than 30 days.

¹ As far as we have been able to determine, ECPA warrants presented to Magistrate Judge Deborah A. Robinson and to Chief Judge Royce C. Lamberth since July 21, 2010, did not have the delayed notification box checked. See Case No. 10-400-M-01; Case No. 10-408-M-01; and Case No. 10-456-M-01. We are unaware of any ECPA warrant presented to Magistrate Judge Facciola since July 21, 2010.

We note, however, that during June 2010 Magistrate Judge Facciola signed five ECPA warrants without checking the delayed notification box. See Case No. 10-331-M-01; Case No. 10-347-M-01; Case No. 10-348-M-01; Case No. 10-349-M-01; and Case No. 10-350-M-01. Likewise, during June 2010 Magistrate Judge Robinson signed three ECPA warrants, and Chief Judge Lamberth signed one, without checking the delayed notification box. See Case No. 10-299-M-01; Case No. 10-300-M-01; Case No. 10-302-M-01; and Case No. 10-359-M-01.

UNDER SEAL

Following are the dates of issuance of all fifteen ECPA warrants, and the delayed notification periods ordered:

Case No. 10-291-M-01	5/28/10	30 days
Case No. 10-423-M-01	8/4/10	30 days
Case No. 10-424-M-01	8/4/10	30 days
Case No. 10-425-M-01	8/4/10	30 days
Case No. 10-429-M-01	8/5/10	90 days
Case No. 10-430-M-01	8/5/10	90 days
Case No. 10-431-M-01	8/5/10	90 days
Case No. 10-432-M-01	8/5/10	90 days
Case No. 10-433-M-01	8/5/10	90 days
Case No. 10-434-M-01	8/5/10	90 days
Case No. 10-435-M-01	8/5/10	90 days
Case No. 10-436-M-01	8/5/10	90 days
Case No. 10-437-M-01	8/5/10	90 days
Case No. 10-438-M-01	8/5/10	90 days
Case No. 10-442-M-01	8/9/10	60 days

The delayed notification period for the first warrant has passed. The delayed notification period for the next three warrants will expire on September 3, 2010. The delayed notification period for the remainder will continue until early October 2010 (in one case) or November 2010.

As is the general practice with ECPA warrants, the Government's applications sought the sealing of the application and the warrant, and no notification to the subscriber or customer of

UNDER SEAL

the e-mail account that was the subject of the application. If the Chief Judge of this Court resolves the Government's Motion for Review in the Government's favor, then no notification will be required. The Government submits that until the Motion for Review is resolved, the Court should stay the notification orders so that the Government is not required to disclose improvidently the existence and nature of the warrants to those whose e-mail accounts have been the subject of the ECPA warrants. Accordingly, the Government seeks entry of the proposed Order, submitted herewith, staying the effect of the delayed notification orders on each of the fifteen ECPA warrants listed herein, *nunc pro tunc* to the date of expiration of the delayed notification period where applicable.

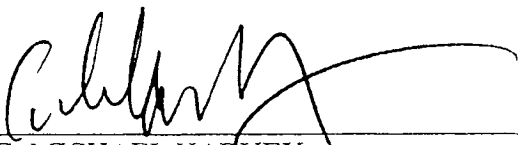
III. CONCLUSION

Wherefore, the Government respectfully requests that the Court issue the proposed Order, staying any notice obligation imposed in the above-listed cases, until ten days after the Chief Judge issues a ruling on the Government's Motion for Review of the Magistrate Judge's July 21, 2010 Memorandum Order.

Respectfully submitted,

RONALD C. MACHEN JR.
UNITED STATES ATTORNEY

By:



G. MICHAEL HARVEY
Assistant United States Attorney
D.C. Bar Number 447-465
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-439
Washington, D.C. 20530

UNDER SEAL

Phone: (202) 305-4155
Michael.Harvey2@usdoj.gov



JONATHAN M. MALIS
Assistant United States Attorney
D.C. Bar Number 454-548
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-447
Washington, D.C. 20530
Phone: (202) 305-9665
Jonathan.M.Malis@usdoj.gov

Dated: September 3, 2010

EXHIBIT N

UNDER SEAL

Case No. 10-432-M-01

Case No. 10-433-M-01

Case No. 10-434-M-01

Case No. 10-435-M-01

Case No. 10-436-M-01

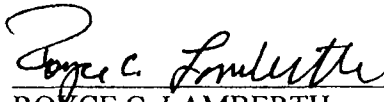
Case No. 10-437-M-01

Case No. 10-438-M-01

Case No. 10-442-M-01;

IT IS FURTHER ORDERED that the stay shall be *nunc pro tunc* to the date of the expiration of the delayed notification period on each ECPA warrant, where such date has passed;

IT IS FURTHER ORDERED that the Government's Motion and this Order shall remain under seal pending further Order of the Chief Judge of this Court.



ROYCE C. LAMBERTH
CHIEF JUDGE
UNITED STATES DISTRICT COURT

cc: G. Michael Harvey
Jonathan M. Malis
Assistant United States Attorneys
National Security Section
555 4th Street, N.W., 11th Floor
Washington, D.C. 20530

EXHIBIT O

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FILED

SEP 20 2010

Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

APPLICATION FOR WARRANT
FOR E-MAIL ACCOUNT
Redacted @GMAIL.COM
MAINTAINED ON COMPUTER SERVERS
OPERATED BY GOOGLE, INC.,
HEADQUARTERED AT
1600 AMPHITHEATRE PARKWAY,
MOUNTAIN VIEW, CA

Maj. No. 10-291-M-01
(AK/JMF/RCL)

UNDER SEAL

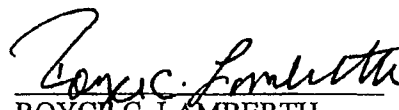
ORDER

On this Court's motion, it is hereby ORDERED that within 14 days the government file a proposed redacted version of the Court's September 20, 2010 Memorandum and Order that could be unsealed with the name of the subpoenaed account and any further identifying information redacted.

SO ORDERED.

Date

9/20/10


ROYCE C. LAMBERTH
Chief Judge
United States District Court

U.S. District and Bankruptcy Courts
for the District of Columbia

A TRUE COPY

ANGELA D. CAESAR, Clerk

By

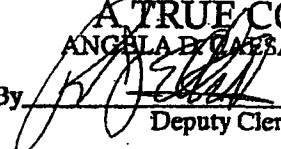

Deputy Clerk

EXHIBIT P

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR WARRANT)	
FOR E-MAIL ACCOUNT)	Mag. No.: 10-291-M-01
██████████@GMAIL.COM)	(AK/JMF/RCL)
MAINTAINED ON COMPUTER SERVERS)	
OPERATED BY GOOGLE, INC.,)	<u>UNDER SEAL</u>
HEADQUARTERED AT)	
1600 AMPHITHEATRE PARKWAY,)	
MOUNTAIN VIEW, CA)	

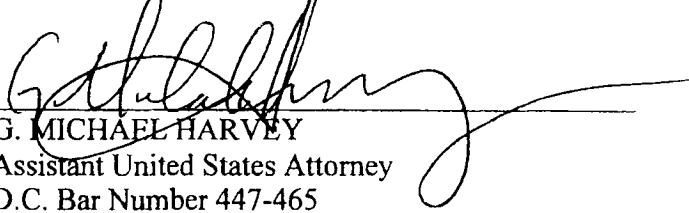
PROPOSED REDACTED MEMORANDUM AND ORDER


In response to the Court's September 20th Order in this matter, the United States, by and through the United States Attorney for the District of Columbia, hereby respectfully provides the Court with the Government's proposed redacted version of the Court's September 20, 2010 Memorandum and Order for purposes of unsealing. The proposed redacted version is attached hereto.

Respectfully submitted,

RONALD C. MACHEN JR.
UNITED STATES ATTORNEY
D.C. Bar Number 447-889

By:


G. MICHAEL HARVEY
Assistant United States Attorney
D.C. Bar Number 447-465
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-439
Washington, D.C. 20530
Phone: (202) 305-4155
Michael.Harvey2@usdoj.gov


JONATHAN M. MALIS
Assistant United States Attorney
D.C. Bar Number 454-548
National Security Section

UNDER SEAL

United States Attorney's Office
555 4th Street, N.W., Room 11-447
Washington, D.C. 20530
Phone: (202) 305-9665
Jonathan.M.Malis@usdoj.gov

Dated: September 30, 2010

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FILED

SEP 20 2010

Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

APPLICATION FOR WARRANT
FOR E-MAIL ACCOUNT
[REDACTED]@GMAIL.COM
MAINTAINED ON COMPUTER SERVERS
OPERATED BY GOOGLE, INC.,
HEADQUARTERED AT
1600 AMPHITHEATRE PARKWAY,
MOUNTAIN VIEW, CA

Maj. No. 10-291-M-01
(AK/JMF/RCL)

UNDER SEAL

MEMORANDUM AND ORDER

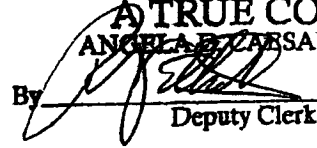
Before the Court is the government's Motion for Review of Magistrate Judge's July 21, 2010 Memorandum Order Regarding Notice Obligations for E-Mail Warrants Issued Under ECPA. Upon consideration of the government's motion and the July 21, 2010 Memorandum Order, the motion will be GRANTED and the Memorandum Order will be REVERSED.

I. BACKGROUND

On May 28, 2010, the government applied for a warrant under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2710 ("ECPA"), to compel the disclosure of certain limited contents of the e-mail account [REDACTED]@gmail.com, maintained by Google, Inc. ("Google"). Magistrate Judge Alan Kay reviewed and issued the warrant. In so doing, Magistrate Judge Kay checked the box on the face of the warrant form allowing for delayed notification under 18 U.S.C. § 3103a. The government had not requested delayed notification in its warrant application. On June 8, 2010, the government filed a Motion for Clarification seeking to clarify Magistrate Judge Kay's intent in checking the box.

U.S. District and Bankruptcy Courts
for the District of Columbia

A TRUE COPY
ANGELA B. CAESAR, Clerk

By  Deputy Clerk

On July 21, 2010, Magistrate Judge John Facciola entered a Memorandum Order adjudicating the government's Motion for Clarification. In his Memorandum Order, Magistrate Judge Facciola held that the government was obligated to notify the subscriber or customer of the e-mail account subject to the FCPA warrant. The government believed that Magistrate Judge Kay had already adjudicated its Motion for Clarification.¹ Accordingly, on July 23, 2010, the government filed a motion to vacate, or in the alternative, for reconsideration of Magistrate Judge Facciola's Memorandum Order ("Motion to Vacate"). In the Motion to Vacate, the government also sought an order staying the unsealing of the Memorandum Order pending adjudication of the Motion to Vacate and its further review, if necessary, by this Court.

On August 4, 2010, while the Motion to Vacate was pending, the government sought an enlargement of time to seek this Court's review of the Memorandum Order until fourteen days after adjudication of the Motion to Vacate. On August 5, 2010, this Court granted that motion. This Court also granted the government's request that the Memorandum Order, Motion to Vacate, Motion for Enlargement, and any adjudication of the Motion to Vacate remain sealed pending the Court's review.

On August 23, 2010, Magistrate Judge Facciola issued a Minute Order denying the government's Motion to Vacate. The order indicates that Magistrate Judge Facciola consulted with Magistrate Judge Kay, who believed that the government "would still provide notice to the subscriber, regardless of whether it was delayed." The order states that Magistrate Judge Kay

¹ On June 17, 2010, having reviewed the government's Motion for Clarification, Magistrate Judge Kay contacted Gregg Maisel, then-acting Chief of the National Security Section of the United States Attorney's Office ("USAO"). According to the government, Magistrate Judge Kay indicated that he had checked the box on the face of the warrant in error and believed that the government had no notice obligation. Magistrate Judge Kay asked the USAO to submit a copy of the warrant with his original signature, which he would correct. On June 21, 2010, Chief Maisel returned the original warrant to Magistrate Judge Kay. Magistrate Judge Kay marked "checked in error AK" next to the delayed notification provision and returned the warrant to the USAO.

withdrew the delayed notice because he believed that the government “would notify the subscriber without delay.” The order further states that Magistrate Judge Kay agreed with the analysis in Magistrate Judge Facciola’s Memorandum Order.

The government does not seek further review of its Motion to Vacate. Rather, it seeks review and reversal of the Memorandum Order on its merits. The government offers three grounds for reversal: (1) that the Memorandum Order is contrary to the plain language of the ECPA’s notice provisions and the government’s obligations under those provisions; (2) that the ECPA provisions regarding warrants for the compelled disclosure of electronic communications do not incorporate the provisions of Fed. R. Crim. P. 41(f)(1)(C); and (3) that Rule 41(f)(1)(C), even assuming it is incorporated into the ECPA, is satisfied by providing notice to the third party, typically an Internet Service Provider (“ISP”), from whom the disclosure is compelled pursuant to an ECPA warrant.

This Court finds that Section 2703(b)(1)(A) of the ECPA incorporates all procedural aspects of Rule 41, including Rule 41(f)(1)(C). The Court finds, however, that Rule 41(f)(1)(C) is satisfied by leaving a copy of the warrant with a third-party ISP. Accordingly, the Court grants the government’s motion for review and reverses the July 21, 2010 Memorandum Order.

II. DISCUSSION

The warrant at issue sought the contents of an e-mail account maintained by Google. The government applied for this warrant under Section 2703(b)(1)(A) of the ECPA.² Section 2703(b)(1) provides that:

A governmental entity may require a provider of remote computing service³ to disclose the contents of any wire or electronic communication

² Section 2703(b) pertains to compelled disclosure by a provider of remote computing service. Section 2703(a) pertains to compelled disclosure by a provider of electronic communication service.

to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

The government contends that Section 2703(b)(1)(A)'s plain language does not require notice to the subscriber or customer whose communications are subject to an ECPA warrant. As the government argues, only Section 2703(b)(1)(B), which pertains to compelled disclosure through the use of an administrative subpoena or court order, requires prior notice.

The government's argument falls short. Under Section 2703(b)(1)(A), a governmental entity seeking compelled disclosure must "obtain[] a warrant issued using the procedures described in the Federal Rules of Criminal Procedure." Specifically, Rule 41 pertains to the issuance of warrants. Thus, the questions before the Court are (1) whether Rule 41(f)(1)(C)

³ The ECPA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). An "electronic communications system" is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." Id. § 2510(14).

applies to warrants issued under Section 2703(b)(1)(A), and (2) if so, whether Rule 41(f)(1)(C) is satisfied by leaving a copy of the warrant with a third-party ISP.

A. Application of Rule 41 to Section 2703(b)(1)(A)

The Court's analysis must begin with the statutory text. Prior to 2001, the ECPA permitted a governmental entity to require the disclosure of electronic communications if the governmental entity obtained "a warrant *issued under* the Federal Rules of Criminal Procedure." 18 U.S.C. § 2703(b)(1)(A) (1998) (emphasis added), amended by Pub. L. No. 107-56, § 220(a)(1). In 2001, the USA PATRIOT Act amended the ECPA to permit compelled disclosure if a governmental entity obtains "a warrant *issued using the procedures described* in the Federal Rules of Criminal Procedure." Id. § 2703(b)(1)(A) (2009) (emphasis added).⁴

The plain language of amended Section 2703(b)(1)(A) incorporates the procedural, not substantive, provisions of Rule 41. Other courts have reached this conclusion with regard to Section 2703(a), which includes the same amended language as Section 2703(b)(1)(A).⁵ See, e.g., *In the Matter of the Application of the United States of America for a Search Warrant*, 665 F. Supp. 2d 1210, 1217 (D. Or. 2009); *In re Search of Yahoo, Inc.*, No. 07-3194-MB, 2007 WL 1539971, at *6 (D. Ariz. May 21, 2007).

The inquiry does not end there, however. Rule 41's procedural provisions relate both to the issuance and execution of a warrant. The government contends that Section 2703(b)(1)(A) incorporates only those procedural provisions of Rule 41 that relate to the *issuance* of a warrant (i.e., Rules 41(d) and 41(e)). The government thus argues that Rule 41(f), which relates to the

⁴ The PATRIOT Act made the same amendment to Section 2703(a).

⁵ For our purposes, the distinction between Sections 2703(a) and 2703(b)(1)(A) is not relevant. Both subsections contain the same amended language directing that warrants be "issued using the procedures described in the Federal Rules of Criminal Procedure." See 18 U.S.C. §§ 2703(a), 2703(b)(1)(A).

execution and *return* of a warrant, does not apply to Section 2703(b)(1)(A). In contrast, Magistrate Judge Facciola's Memorandum Opinion reads Section 2703(b)(1)(A) to incorporate Rule 41's provisions, including Rule 41(f)(1)(C).

Neither the ECPA's text nor its legislative history indicate the extent to which Rule 41's procedures have been incorporated. *See* S. Rep. No. 99-541, at 37 (1986) (summarizing Section 2703's text without additional explanation). Indeed, it is reasonable to read the language "issued using the procedures described in the Federal Rules of Criminal Procedure" to support either a limited or wholesale incorporation of Rule 41's procedures. Among those courts to have considered the applicability of Rule 41 to Section 2703(a), none have faced the question of which procedural provisions have been incorporated.⁶

The government contends that it would be incongruous to apply Rule 41(f) to ECPA warrants. It argues that Rule 41(f) describes steps a law enforcement officer must take while present for the execution of a search warrant, whereas the presence of a law enforcement officer "shall not be required for service or execution" of ECPA warrants. 18 U.S.C. § 2703(g). But it is unsurprising that some provisions applicable to ordinary search warrants do not fit neatly into Section 2703. Thus, the government's argument does not weigh strongly in favor of the limited view it asks the Court to adopt.

⁶ Rather, these courts have determined that Rule 41(b) is substantive and thus inapplicable to ECPA warrants. *See, e.g., United States v. Berkos*, 543 F.3d 392, 392 (7th Cir. 2008); *In re Search of Yahoo, Inc.*, No. 07-3194-MB, 2007 WL 1539971, at *7 (D. Ariz. May 21, 2007); *In re Search Warrant*, No. 6:05-MC-168-Orl-31JGG, 2005 WL 3844032, at *6 (M.D. Fla. Feb. 13, 2006); *United States v. Kernell*, No. 3:08-CR-142, 2010 WL 1408437, at *4 (E.D. Tenn. 2010).

In the absence of textual or legislative guidance, this Court concludes that all of Rule 41's procedural provisions apply to Section 2703(b)(1)(A), including Rule 41(f)(1)(C). As described below, however, 41(f)(1)(C) is satisfied by leaving a copy of the warrant with a third-party ISP.

B. The Government's Obligations under Rule 41(f)(1)(C)

Magistrate Judge Facciola's Memorandum Order refers to "the notice thus required by Rule 41." Mem. Order at 7. As the government notes, however, the relevant portion of Rule 41 does not include the word "notice." Rather, Rule 41(f)(1)(C) requires that:

The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property.

Rule 41 thus allows an officer to give a copy of the warrant and a receipt to the person from whose premises the property is taken, even if that person does not own the property. There is no separate requirement that the property's owner receive a copy of the warrant, a receipt, or any other form of notice. Thus, the Eighth Circuit found that police complied with a state rule of criminal procedure virtually identical to Rule 41(f) when they left a copy of their warrant and a receipt at the Federal Express facility from which they had seized a package. *United States v. Zacher*, 465 F.3d 336, 339 (8th Cir. 2006). The court held that it was therefore "immaterial" to notify the defendant of the seizure. *Id.*

Analogizing to *Zacher*, the district court in *In the Matter of the Application of the United States of America for a Search Warrant* found that the government satisfied Rule 41(f)(1)(C) by serving an ECPA warrant on third-party ISPs. As the court explained:

The ISPs are analogous to FedEx in *Zacher*; the electronic information was stored on the servers at Google and Webhost the same way the package was stored at FedEx. Requiring notice to the subscriber ignores

this third-party context. When the property to be seized is in the possession of a third party, Rule 41(f)(1)(C) requires no more than what was already accomplished in this case.

665 F. Supp. 2d at 1221–22. Similarly, in this case, the government served its warrant on Google, a third-party ISP. In so doing, the government satisfied Rule 41(f)(1)(C). Accordingly, even under a reading of Section 2703(b)(1)(A) that incorporates Rule 41(f), the government has no further obligation to notify the subscriber of the e-mail account at issue.

III. CONCLUSION AND ORDER

For the reasons discussed above, it is hereby

ORDERED that the government's Motion for Review is **GRANTED**; and it is

FURTHER ORDERED that the Magistrate Judge's July 21, 2010 Memorandum Order is **REVERSED**; and it is

FURTHER ORDERED that the government is not required to give notice to the subscriber or customer of an e-mail account whose account is the subject of a warrant issued under the Electronic Communications Privacy Act, §§ 2701-2710; and it is

FURTHER ORDERED that the Clerk's office shall not make any entry on the public docket in this case of the government's Motion for Review and this Order granting such motion, until further order of this Court.

SO ORDERED this 20th day of September 2010.



ROYCE C. LAMBERTH
Chief Judge
United States District Court

EXHIBIT Q

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR WARRANT
FOR E-MAIL ACCOUNT
[REDACTED]@GMAIL.COM
MAINTAINED ON COMPUTER SERVERS
OPERATED BY GOOGLE, INC.,
HEADQUARTERED AT
1600 AMPHITHEATRE PARKWAY,
MOUNTAIN VIEW, CA

Mug.
Maj. No. 10-291-M-01
(AK/JMF/RCL)

FILED

NOV - 1 2010

Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

ORDER

The Court's September 20, 2010 Memorandum and Order in this matter, which was previously sealed, is being released in redacted form for the benefit of the public. The name of the subpoenaed e-mail account has been redacted. Accordingly, it is hereby ordered that the redacted opinion attached hereto be unsealed and placed on the public record.

SO ORDERED this 1st day of November 2010.



ROYCE C. LAMBERTH
Chief Judge
United States District Court

EXHIBIT R

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT)
FOR E-MAIL ACCOUNT)
[REDACTED]@GMAIL.COM)
MAINTAINED ON COMPUTER SERVERS)
OPERATED BY GOOGLE, INC.,)
HEADQUARTERED AT)
1600 AMPHITHEATRE PARKWAY,)
MOUNTAIN VIEW, CA)

Mag. No.: 10-291-M-01

UNDER SEAL

FILED

**GOVERNMENT'S MOTION FOR UNSEALING OF SEARCH WARRANT AND
RELATED MATERIALS**

The United States, by and through its attorney, the United States Attorney for the District of Columbia, respectfully requests the Court to unseal in the above-captioned matter: (1) the application for search warrant, (2) the affidavit in support of the application for search warrant, (3) the search and seizure warrant, and (4) the Attachment A thereto (hereinafter "search warrant material"). The Government seeks the unsealing of the search warrant material to fulfill its discovery obligations in a pending criminal case, United States v. Stephen Jin-Woo Kim, Cr. No. 10-225 (CKK), to which the search warrant relates. See F.R.Cr.P. 12(b)(4). To protect the privacy of those involved, the Government requests that dates of birth and email addresses appearing in the search warrant material be redacted before it is placed on the public record. Cf. F.R.Cr. P. 49. To assist the Court, and consistent with F.R.Cr.P. 49.1(d), the Government attaches hereto redacted versions of the search warrant material for entry on the public docket. Further, the Government requests that it be permitted to produce to the defense in United States v. Stephen Jin-Woo Kim unredacted versions of the search warrant material pursuant to the Rule 16 Protective Order entered in that matter on October 13, 2010. See United States v. Stephen Jin-Woo Kim, Cr. No. 10-225 (CKK), Docket #11.

A proposed Order is submitted herewith this motion.

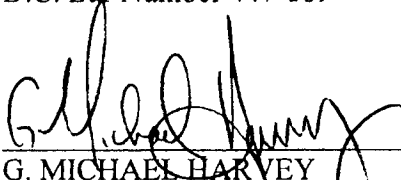
WHEREFORE, the Government respectfully requests (1) that the application for search

warrant in this matter, the affidavit in support of the application for search warrant, the search and seizure warrant, and the Attachment A thereto, be unsealed; (2) that the attached redacted versions of the search warrant material be placed on the public record; and (3) that the Government be permitted to produce unredacted versions of the search warrant material to the defense in United States v. Stephen Jin-Woo Kim pursuant to the Rule 16 Protective Order in that matter.


Respectfully submitted,

RONALD C. MACHEN JR.
UNITED STATES ATTORNEY
D.C. Bar Number 447-889

By:



G. MICHAEL HARVEY
Assistant United States Attorney
D.C. Bar Number 447-465
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-848
Washington, D.C. 20530
Phone: (202) 252-7810
Michael.Harvey@usdoj.gov



JONATHAN M. MALIS
Assistant United States Attorney
D.C. Bar Number 454-548
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-447
Washington, D.C. 20530
Phone: (202) 252-7806
Jonathan.M.Malis@usdoj.gov



Handwritten signature of Deborah Curtis, with the initials 'CMA' written to the right of the signature.

DEBORAH CURTIS

Trial Attorney

CA Bar Number 172208

Counterespionage Section

U.S. Department of Justice

600 E Street, N.W.

Washington, D.C. 20530

Phone: (202) 233-2133

Deborah.Curtis@usdoj.gov

Attachment A

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)E-mail Account [REDACTED]@gmail.com on
Computer Servers Operated by Google, Inc., 1600
Amphitheatre Parkway, Mountain View, California

Case No.

70-291-M-07

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
e-mail account [REDACTED]@gmail.com, maintained on computer servers operated by Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, California,

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

certain property, the disclosure of which is governed by Title 42, U.S.C. Section 2000aa, and Title 18, U.S.C. Sections 2701 through 2711, namely contents of electronic e-mails and other electronic data and more fully described in ATTACHMENT A to this application.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 793	Gathering, transmitting or losing defense information

The application is based on these facts:
See attached affidavit herein incorporated by reference as if fully restated herein.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Reginald B. Reyes, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: MAY 28 2010

City and state: Washington, D.C.

Judge's Signature

ALAN KAY

U.S. MAGISTRATE JUDGE

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of ColumbiaIn the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))

Case No. 10-291-M-01

E-mail Account [REDACTED]@gmail.com on)
Computer Servers Operated by Google, Inc., 1600)
Amphitheatre Parkway, Mountain View, California)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
(Identify the person or describe the property to be searched and give its location):
E-mail account [REDACTED]@gmail.com, maintained on computer servers operated by Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the property to be seized):
Certain property, the disclosure of which is governed by Title 42, U.S.C. Section 2000aa, and Title 18, U.S.C. Sections 2701 through 2711, namely contents of electronic e-mails and other electronic data, more fully described in ATTACHMENT A to this application.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before

JUN 11 2010

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

(name)

☒ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for 30 days (not to exceed 30).

☐ Until, the facts justifying, the later specific date of _____.

Date and time issued: MAY 28 2010

City and state: District of Columbia

ALAN RAY
U.S. MAGISTRATE JUDGE

Printed name and title

ATTACHMENT A: ITEMS TO BE SEIZED

Pursuant to 18 U.S.C. § 2703 and 42 U.S.C. § 2000aa(a), it is hereby ordered as follows:

I. SERVICE OF WARRANT AND SEARCH PROCEDURE

a. Google, Incorporated, a provider of electronic communication and remote computing services, located at 1600 Amphitheatre Parkway, Mountain View, California, (the "PROVIDER") will isolate those accounts and files described in Section II below. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

b. The PROVIDER shall not notify any other person, including the subscriber(s) of [REDACTED]@gmail.com of the existence of the warrant.

c. In order to minimize any disruption of computer service to innocent third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

d. As soon as practicable after service of this warrant, the PROVIDER shall provide the exact duplicate in electronic form of the account and files described in Section II below and all information stored in that account and files to the following FBI special agent:

Reginald B. Reyes
FBI-WFO
601 4th Street, NW
Washington, D.C. 20535
Fax: 202-278-2864
Desk: 202-278-4868

The PROVIDER shall send the information to the agent via facsimile and overnight mail, and where maintained in electronic form, on CD-ROM or an equivalent electronic medium.

e. The FBI will make an exact duplicate of the original production from the PROVIDER. The original production from the PROVIDER will be sealed by the FBI and preserved for authenticity and chain of custody purposes.

II. FILES AND ACCOUNTS TO BE COPIED BY THE PROVIDER'S EMPLOYEES

a. Any and all communications, on whatever date, between

██████████@gmail.com ("SUBJECT ACCOUNT") and any of the following accounts:

- (1) ██████████@yahoo.com,
- (2) ██████████@yahoo.com, and
- (3) ██████████@gmail.com.

"Any and all communications" includes, without limitation, received messages (whether "to," "cc'd," or "bcc'd" to the SUBJECT ACCOUNT), forwarded messages, sent messages (whether "to," "cc'd," or "bcc'd" to the three above-listed accounts), deleted messages, and messages maintained in trash or other folders, and any attachments thereto, including videos, documents, photos, internet addresses, and computer files sent to and received from other websites. "Any and all communications" further includes all prior email messages in an email "chain" between the SUBJECT ACCOUNT and any of the three above-listed accounts, whether or not those prior emails were in fact sent between the SUBJECT ACCOUNT and the above-listed accounts;

b. Any and all communications "to" or "from" the SUBJECT ACCOUNT on June 10 and/or June 11, 2009. "Any and all communications" includes, without limitation, received messages (whether "to," "cc'd," or "bcc'd" to the SUBJECT ACCOUNT), forwarded messages, sent messages, deleted messages, messages maintained in trash or other folders, and any attachments thereto, including videos, documents, photos, internet addresses, and computer files

sent to and received from other websites. "Any and all communications" further includes all prior email messages in an email "chain" sent "to" or "from" the SUBJECT ACCOUNT on June 10 or June 11, 2009, whether or not those prior emails in the "chain" were in fact sent or received on June 10 or June 11, 2009;

c. All existing printouts from original storage of all of the electronic mail described above in Section II (a) and II(b);

d. All transactional information of all activity of the SUBJECT ACCOUNT described above in Section II(a) and II(b), including log files, dates, times, methods of connecting, ports, dial-ups, registration Internet Protocol (IP) address and/or locations;

e. All business records and subscriber information, in any form kept, pertaining to the SUBJECT ACCOUNT described above in Section II(a) and II(b), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, account numbers, screen names, status of accounts, dates of service, methods of payment, telephone numbers, addresses, detailed billing records, and histories and profiles;

f. All records indicating the account preferences and services available to subscribers of the SUBJECT ACCOUNT described above in Section II(a) and II(b).

III. INFORMATION TO BE SEIZED BY LAW ENFORCEMENT PERSONNEL

Items to be seized, which are believed to be evidence and fruits of violations of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information) as follows:

a. The contents of electronic communications, including attachments and stored files, for the SUBJECT ACCOUNT as described and limited by Section II(a) and II(b) above,

including videos, computer files sent to and received from other websites, received messages, sent messages, deleted messages, messages maintained in trash or other folders, any attachments thereto, and all existing printouts from original storage of all of the electronic mail described above in Section II(a) and II(b), that pertain to:

1. records or information related to violations of 18 U.S.C. § 793;
2. any and all communications between Stephen Kim and the author of the article (the "Author") that is the subject matter of the FBI investigation that is the basis for this warrant (the "Article") and any record or information that reflects such communications;
3. records or information relating to Stephen Kim's communications and/or activities on the date of publication of the Article;
4. records or information relating to the Author's communication with any other source or potential source of the information disclosed in the Article;
5. records or information related to Stephen Kim's or the Author's knowledge of laws, regulations, rules and/or procedures prohibiting the unauthorized disclosure of national defense or classified information;
6. records or information related to Stephen Kim's or the Author's knowledge of government rules and/or procedures regarding communications with members of the media;
7. records or information related to any disclosure or prospective disclosure of classified and/or intelligence information;
8. any classified document, image, record or information, and any

communications concerning such documents, images, records, or information;

9. any document, image, record or information concerning the national defense, including but not limited to documents, maps, plans, diagrams, guides, manuals, and other Department of Defense, U.S. military, and/or weapons material, as well as sources and methods of intelligence gathering, and any communications concerning such documents, images, records, or information;
10. records or information related to the state of mind of any individuals seeking the disclosure or receipt of classified, intelligence and/or national defense information;
11. records or information related to the subject matter of the Article; and
12. records or information related to the user(s) of the SUBJECT ACCOUNT.

b. All of the records and information described above in Sections II(d), II(e), and II(f) including:

1. Account information for the SUBJECT ACCOUNT including:
 - (a) Names and associated email addresses;
 - (b) Physical address and location information;
 - (c) Records of session times and durations;
 - (d) Length of service (including start date) and types of service utilized;
 - (e) Telephone or instrument number or other subscriber number or identity,

including any temporarily assigned network address;

(f) The means and source of payment for such service (including any credit card or bank account number); and

(g) Internet Protocol addresses used by the subscriber to register the account or otherwise initiate service.

2. User connection logs for the SUBJECT ACCOUNT for any connections to or from the SUBJECT ACCOUNT. User connection logs should include the following:

- (a) Connection time and date;
- (b) Disconnect time and date;
- (c) Method of connection to system (e.g., SLIP, PPP, Shell);
- (d) Data transfer volume (e.g., bytes);
- (e) The IP address that was used when the user connected to the service,
- (f) Connection information for other systems to which user connected via the SUBJECT ACCOUNT, including:

- (1) Connection destination;
- (2) Connection time and date;
- (3) Disconnect time and date;
- (4) Method of connection to system (e.g., telnet, ftp, http);
- (5) Data transfer volume (e.g., bytes);
- (6) Any other relevant routing information.

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT)
FOR E-MAIL ACCOUNT)
[REDACTED]@GMAIL.COM)
MAINTAINED ON COMPUTER SERVERS)
OPERATED BY GOOGLE, INC.,)
HEADQUARTERED AT)
1600 AMPHITHEATRE PARKWAY,)
MOUNTAIN VIEW, CA)

M-9.
Misc. No.: 10-291-M-01

UNDER SEAL

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, Reginald B. Reyes, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the Washington Field Office, and have been employed by the FBI for over five years. I am assigned to a squad responsible for counterespionage matters and matters involving the unauthorized disclosure of classified information, and have worked in this field since October 2005. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure of classified information, I am familiar with the tactics, methods, and techniques of particular United States persons who possess, or have possessed a United States government security clearance and may choose to harm the United States by misusing their access to classified information. Before working for the FBI, I was a Special Agent with the Drug Enforcement Administration for two years.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

The statements in this affidavit are based in part on information provided by the investigation to date and on my experience and background as a Special Agent of the FBI. The information set forth in this affidavit concerning the investigation at issue is known to me as a result of my own involvement in that investigation or has been provided to me by other law enforcement professionals. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

3. This affidavit is made in support of an application for a warrant pursuant to 18 U.S.C. § 2703 and 42 U.S.C. § 2000aa to compel Google, Incorporated, which functions as an electronic communication service and remote computing service, and is a provider of electronic communication and remote computing services (hereinafter "Google" or the "PROVIDER"), located at 1600 Amphitheatre Parkway, Mountain View, California, to provide subscriber information, records, and the contents of limited wire and electronic communications pertaining to the account identified as [REDACTED]@gmail.com, herein referred to as the SUBJECT ACCOUNT. I have been informed by the United States Attorney's Office that because this Court has jurisdiction over the offense under investigation, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. § 2703(a).¹

4. The SUBJECT ACCOUNT is an e-mail account. As discussed below, investigation into the SUBJECT ACCOUNT indicates it is an e-mail account used by a national news reporter (hereinafter "the Reporter").

¹ See 18 U.S.C. § 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation . . .").

5. For the reasons set forth below, I believe there is probable cause to conclude that the contents of the wire and electronic communications pertaining to the SUBJECT ACCOUNT, are evidence, fruits and instrumentalities of criminal violations of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information), and that there is probable cause to believe that the Reporter has committed or is committing a violation of section 793(d), as an aider and abettor and/or co-conspirator, to which the materials relate.

6. Based on my training and experience, and discussions with the United States Attorney's Office, I have learned that Title 18, United States Code, Section 793(d) makes punishable, by up to ten years imprisonment, the willful communication, delivery or transmission of documents and information related to the national defense to someone not entitled to receive them by one with lawful access or possession of the same. Specifically, section 793(d) states:

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(d). Further, section 793(g) makes a conspiracy to violate section 793(d) a violation of 793 and punishable by up to ten years imprisonment. See 18 U.S.C. § 793(g).

7. Based on my training and experience, and discussion with the United States

Attorney's Office, I have learned that "classified" information is defined by Executive Order 12958, as amended by Executive Order 13292, and their predecessor orders, Executive Orders 12356 and 12065, as information in any form that: (1) is owned by, produced by or for, or under control of the United States government; (2) falls within one or more of the categories set forth in the Order; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such damage could reasonably result in "exceptionally grave" damage to the national security, the information may be classified as "TOP SECRET." Access to classified information at any level may be further restricted through compartmentalization "SENSITIVE COMPARTMENTED INFORMATION" (SCI) categories, which further restricts the dissemination and handling of the information.

8. Based on my training and experience, and discussions with the United States Attorney's Office, I have learned that the Privacy Protection Act (the "PPA"), codified at 42 U.S.C. § 2000aa et seq., defines when a search warrant impacting media-related work product and documentary materials may be executed. Section 2000aa(a) of the PPA states, in pertinent part:

(a) Work product materials

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any *work product materials*² possessed by a person reasonably

² Section 2000aa-7(b) defines the terms "documentary materials" as follows:

(b) "Work product materials", as used in this chapter, means materials, other than contraband or the fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or which is or has been used, as a means of committing a criminal offense, and –

believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if—

- (1) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section 793, 794, 797, or 798 of *title 18*, or [other enumerated statutes])

(b) Other documents

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize *documentary materials, other than work product materials*,³ possessed

-
- (1) in anticipation of communicating such materials to the public, are prepared, produced, authored, or created, whether by the person in possession of the materials or by any other person;
 - (2) are possessed for the purposes of communicating such materials to the public; and
 - (3) include mental impressions, conclusions, opinions, or theories of the person who prepared, produced, authored or created such material.

42 U.S.C. § 2000aa-7(b).

³ Section 2000aa-7(a) defines the terms “documentary materials” as follows:

- (a) “Documentary materials”, as used in this chapter, means materials upon which information is recorded, and includes, but is not limited to, written or printed materials, photographs, motion picture films, negatives, video tapes, audio tapes, and other mechanically, magnetically or electronically recorded cards, tapes, or discs, but does not include contraband or fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or

by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if—

- (1) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section 793, 794, 797, or 798 of *title 18*, or [other enumerated statutes]) ...

42 U.S.C. § 2000aa(a) (emphasis added). Thus, section 2000aa(a) specifically exempts from its prohibitions cases in which there is probable cause to believe that the possessor of media related work product or documentary materials has committed a violation of section 793. I have been further informed that the legislative history of the statute indicates:

The purpose of the statute is to limit searches for materials held by persons involved in First Amendment activities who are themselves not suspected of participation in the criminal activity for which the materials are sought, and not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation.

S. Rep. No. 96-874 at 11 (1980), reprinted in 1980 U.S.C.C.A.N. 3950. I also have been informed that violations of the PPA do not result in suppression of the evidence, see 42 U.S.C. §

which is or has been used as, the means of committing a criminal offense.

42 U.S.C. § 2000aa-7(a).

2000aa-6(d), but can result in civil damages against the sovereign whose officers or employees executed the search in violation of section 2000aa(a). See 42 U.S.C. § 2000aa-6(a).

II. FACTS SUPPORTING PROBABLE CAUSE

9. In or about June 2009, classified United States national defense information was published in an article on a national news organization's website (hereinafter the "June 2009 article"). The June 2009 article was written by the Reporter who frequently physically worked out of a booth located at the main Department of State (DoS) building located at 2201 C Street, N.W., Washington, D.C.

10. The Intelligence Community owner of the classified information at issue (the "Owner") has informed the FBI that the June 2009 article disclosed national defense information that was classified TOP SECRET/SPECIAL COMPARTMENTED INFORMATION (TS/SCI). It has also informed the FBI that the information was not declassified prior to its disclosure in the June 2009 article, that the information's public disclosure has never been lawfully authorized, and that the information remains classified at the TS/SCI level to this day.

11. Following the disclosure of the classified national defense information in the June 2009 article, an FBI investigation was initiated to determine the source(s) of the unauthorized disclosure. That investigation has revealed that the Owner's TS/SCI information disclosed in the June 2009 article was first made available to a limited number of Intelligence Community members in an intelligence report (the "Intelligence Report") that was electronically disseminated to the Intelligence Community outside of the Owner on the morning of the date of

publication of the June 2009 article. The Intelligence Report was accessible on a classified information database that warned all Intelligence Community users seeking access to information in the database, through a "click through" banner, of the following:

Due to recent unauthorized disclosures of sensitive intelligence, you are reminded of your responsibility to protect the extremely sensitive, compartmented intelligence contained in this system. Use of this computer system constitutes consent to monitoring of your actions. None of the intelligence contained in this system may be discussed or shared with individuals who are not authorized to receive it. Unauthorized use . . . is prohibited and violations may result in disciplinary action or criminal prosecution.

12. The Intelligence Report was clearly marked TS/SCI. The security markings further instructed the reader that every portion of the information contained in the Intelligence Report was classified TS/SCI and was not authorized for disclosure without permission of the Owner.

13. The investigation has revealed that one individual who accessed the Intelligence Report through the classified database on the date of the June 2009 article (prior to the publication of the article) was Stephen Jin-Woo Kim.⁴ Review of government records has revealed that Mr. Kim was born on [REDACTED] and was naturalized as a United States

⁴ So far, the FBI's investigation has revealed in excess of 95 individuals, in addition to Mr. Kim, who accessed the Intelligence Report on the date of the June 2009 article and prior to its publication. To date, however, the FBI's investigation has not revealed any other individual, other than Mr. Kim, who *both* accessed the Intelligence Report *and* who also had contact with the Reporter on the date of publication of the June 2009 article. Thus far, the FBI's investigation has revealed four other individuals who have admitted to limited contacts with either the Reporter's news organization or the Reporter anywhere from six weeks, to six months, or to nine years prior to publication of the June 2009 article. The FBI's investigation of these contacts is on-going. All these individuals have denied being the source of the June 2009 article and the FBI has not discovered any information to date that would tend to discredit their statements.

citizen in 1988.⁵ Mr. Kim is a Lawrence Livermore National Laboratory employee who was on detail to the DoS's Bureau of Verification, Compliance, and Implementation (VCI) at the time of the publication of the June 2009 article. VCI is responsible for ensuring that appropriate verification requirements are fully considered and properly integrated into arms control, nonproliferation, and disarmament agreements and to monitor other countries' compliance with such agreements. On his detail to VCI, Mr. Kim worked as a Senior Advisor for Intelligence to the Assistant Secretary of State for VCI.

14. Like the Reporter's booth at DoS on the date of publication of the June 2009 article, Mr. Kim's VCI office was located at the DoS headquarters building at 2201 C Street, N.W., Washington, D.C.

15. Based on my training and experience, I have learned that classified information, of any designation, may be shared only with persons determined by an appropriate United States government official to be eligible for access to classified information, that is, the individual has received a security clearance, has signed an approved non-disclosure agreement and possesses a "need to know" the information in question. If a person is not eligible to receive classified information, classified information may not be disclosed to that person.

16. Government records demonstrate that, at all times relevant to this investigation, Mr. Kim possessed a TS/SCI security clearance. As a government employee with a security clearance, and prior to the disclosures at issue, Mr. Kim executed multiple SF 312 Classified Information Non-Disclosure Agreements (NDAs) with the Government. NDAs are legally

⁵ In prior affidavits in this matter seeking search warrants of Mr. Kim's e-mail accounts, the date of Mr. Kim's naturalization was erroneously reported as 1999 rather than 1988.

binding agreements between an individual being granted, or already in possession of, a security clearance, and the United States Government wherein the parties agree that the individual never disclose classified information without the authorization of the Government. The NDAs further notified Mr. Kim that the unauthorized disclosure of classified information can lead to criminal prosecution, including for violations of 18 U.S.C. § 793.

17. The Reporter did not possess a security clearance and was not entitled to receive the information published in the June 2009 article. Nor was Mr. Kim authorized, directly or indirectly, by the United States Government to deliver, communicate, or transmit the TS/SCI information in the article to the Reporter or any other member of the press.

18. Government electronic records revealed that between the hours the Intelligence Report was made available to the Intelligence Community on the morning of the publication of the June 2009 article, and the publication of the June 2009 article, the unique electronic user profile and password associated with Mr. Kim *accessed at least three times* the Intelligence Report that contained the TS/SCI information which later that day was disclosed in the June 2009 article.⁶ Specifically, the Intelligence Report was accessed by Mr. Kim's user profile at or

⁶ Mr. Kim accessed the classified database in question through his DoS work computer provided to him to process and access TOP SECRET/SCI information. The "click through" banner on Mr. Kim's DoS classified computer permits the government's review of the data contained therein. It read:

NOTICE AND CONSENT LOG-ON BANNER

THIS IS A DEPARTMENT OF STATE (DoS) COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DoS COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED

around 11:27 a.m., 11:37 a.m., and 11:48 a.m. on the date the article was published. DoS security badge access records suggest that, at those times, Mr. Kim was in his VCI office suite where his DoS TS/SCI computer was located on which he would have accessed the Intelligence Report.

19. Telephone call records demonstrate that earlier on that same day, multiple telephone communications occurred between phone numbers associated with Mr. Kim and with the Reporter. Specifically:

- at or around 10:15 a.m., an approximate 34-second call was made from the Reporter's DoS desk telephone to Mr. Kim's DoS desk telephone;
- two minutes later, at or around 10:17 a.m., an approximate 11 minute 35 second call was made from Mr. Kim's DoS desk telephone to the Reporter's DoS desk telephone;

ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DoS ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DoS COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

Further, Mr. Kim had to "click through" *an additional* banner on the classified database where he accessed the Intelligence Report, as detailed in Paragraph 11 above, which stated that "use of this computer system constitutes consent to monitoring of your actions."

Moreover, DoS policy specifically prescribes that "personal use [of DoS classified computers] is strictly prohibited; therefore, users do not have a reasonable expectation of privacy." 12 FAM 632.1.5; 5 FAM 723(2). In addition, the DoS's Foreign Affairs Manual states that DoS office spaces are subject to security inspections to insure that classified information is properly protected. Indeed, Mr. Kim's office was located in a secured facility within the main DoS building that was subject to daily inspections by rotating duty officers (sometimes including Mr. Kim himself) who were responsible for making sure that classified information in each of the offices within the facility was properly secured.

- one hour later, at or around 11:18 a.m., an approximate 3 minute 58 second call was made from Mr. Kim's DoS desk telephone to the Reporter's DoS desk telephone; and
- at or around 11:24 a.m., an approximate 18 second call was made from Mr. Kim's DoS desk telephone to the Reporter's DoS desk telephone.

20. Thereafter, telephone call records for Mr. Kim's office phone reveal that *at or around the same time that Mr. Kim's user profile was viewing the TS/SCI Intelligence Report two telephone calls were placed from his desk phone to the Reporter.* Specifically, a call was made at or around 11:37 a.m (at or around the same time that Mr. Kim's user profile was viewing the Intelligence Report) from Mr. Kim's desk phone to the Reporter's desk phone located within the DoS. That call lasted approximately 20 seconds. Immediately thereafter, a call was placed by Mr. Kim's desk phone to the Reporter's cell phone. This second call lasted approximately 1 minute and 8 seconds.

21. In the hour following those calls, the FBI's investigation has revealed evidence suggesting that Mr. Kim met face-to-face with the Reporter outside of the DoS. Specifically, DoS security badge access records demonstrate that Mr. Kim and the Reporter departed the DoS building at 2201 C Street, N.W., at nearly the same time, they were absent from the building for nearly 25 minutes, and then they returned to the DoS building at nearly the same time.

Specifically, the security badge access records indicate:

- Mr. Kim departed DoS at or around 12:02 p.m. followed shortly thereafter by The Reporter at or around 12:03 p.m.; and
- Mr. Kim returned to DoS at or around 12:26 p.m. followed shortly thereafter by The Reporter at or around 12:30 p.m.

22. Within a few hours after those nearly simultaneous exits and entries at DoS, the

June 2009 article was published on the Internet. Following the publication of the article, yet another call was placed from Mr. Kim's DoS desk telephone to the Reporter's DoS desk telephone number. This call lasted approximately 22 seconds.

23. In the evening of August 31, 2009, DoS Diplomatic Security entered Mr. Kim's DoS office space, without his knowledge, pursuant to DoS internal regulations, procedures, and computer banner authority for purposes of imaging his computer hard drives. Lying in plain view on Mr. Kim's desk next to his DoS computer was a photocopy of the June 2009 article as well as two other articles published in June 2009. All three articles were stapled together. These three articles were also observed on Mr. Kim's desk during entries made in his DoS office space on September 21 and 22, 2009.

24. On September 24, 2009, the FBI conducted a non-custodial interview of Mr. Kim concerning the leak of classified information in the June 2009 article, among other leaks of classified information. During that interview, Mr. Kim denied being a source of the classified information in the June 2009 article. Mr. Kim also claimed to have no recollection of one of the other two articles which were seen in plain view on his desk on August 31, 2009. Mr. Kim admitted to meeting the Reporter in approximately March 2009 but denied having any contact with the Reporter since that time. Mr. Kim acknowledged that DoS protocol required that he would have to go through the DoS press office before he could speak with the press. Mr. Kim stated, "I wouldn't pick-up a phone and call [the Reporter] or [the news organization that the Reporter works for]."

25. An analysis of call records for Mr. Kim's DoS *desk phone* reveals that between May 26, 2009 and July 14, 2009, *36 calls* were placed to or received from telephone numbers

associated with the Reporter, including the 7 aforementioned calls on the date of the publication of the June 2009 article. Further, there were 3 *calls* during this timeframe between his desk phone and a number associated with the Reporter's news organization.

26. During the September 24, 2009 non-custodial interview, when asked by the FBI for a cell phone number to reach him in the future, Mr. Kim stated that his cell phone was "no longer active" as of the day of the interview. Mr. Kim indicated to the FBI that he would be purchasing a new cell phone with a different number.

27. An analysis of call records for Mr. Kim's *cellular phone* reveals that between May 26, 2009 and June 30, 2009, 16 *calls* were placed to or received from telephone numbers associated with the Reporter and 10 *calls*⁷ were placed to or received from telephone numbers associated with the Reporter's news organization.

28. It is apparent from the foregoing both that Mr. Kim was in contact with the Reporter on multiple occasions prior to and after the publication of the June 2009 article, and that Mr. Kim did not want the FBI, who he knew was investigating the leak of classified information in that article, to know about those contacts. The FBI has also learned that, following its interview with Mr. Kim, he provided the Department of Energy (DoE) – for which Mr. Kim's permanent employer, LLNL, is a sub-contractor – with "pre-paid" cell phone number

⁷ In prior affidavits in this matter seeking search warrants of Mr. Kim's e-mail accounts, it was reported that there were 11 calls between Mr. Kim's cellular phone and telephone numbers associated with the Reporter's news organization. Mr. Kim's toll records for his cellular phone do, in fact, list 11 such calls. Further review of those records suggested, however, that one of the calls may have been double counted by Mr. Kim's cellular telephone service provider. Discovering this discrepancy, the service provider was contacted and indicated that what appears to be two calls on the toll records was, in fact, only a single call. Accordingly, in this affidavit, I have corrected the total of the calls between Mr. Kim's cellular telephone and telephone numbers associated with the Reporter's news organization to reflect that there were only 10 such calls.

(sometimes referred to as a “throw away” phone) that he instructed DoE representatives to use in the future to contact him about future employment opportunities.

29. Similarly, during the same September 24, 2009 non-custodial interview, Mr. Kim told the FBI that the best e-mail address through which to contact him was [REDACTED]@yahoo.com. One day later, Mr. Kim e-mailed the FBI and stated that “[m]y yahoo account that I gave you is full and am [sic] going to get rid of it. I can be reached at [REDACTED]@gmail.com.” It is apparent from the foregoing that, like his cell phone number, Mr. Kim was concerned about the FBI focusing on his [REDACTED]@yahoo.com e-mail account.

30. Following the FBI’s interview of Mr. Kim on September 24, 2009, FBI and DoS/Diplomatic Security entered Mr. Kim’s office on the evening of September 26, 2009. The stapled photocopies of the three articles containing classified information (including the June 2009 article) seen next to Mr. Kim’s computer on August 31, 2009, September 21 and 22, 2009, were no longer present in Mr. Kim’s office on September 26th – two days after his interview with the FBI wherein he was questioned about the unauthorized disclosures of classified information in the June 2009 article.

31. A forensic analysis of the hard drive imaged from Mr. Kim’s DoS unclassified DoS computer,⁸ has revealed an e-mail communication, dated July 11, 2009, from the Reporter’s

⁸ The “click through” banner on Mr. Kim’s DoS unclassified computer permits the government’s review of the data contained therein. It reads as follows:

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to the network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary actions, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

- * You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.
- * Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

Nothing herein consents to the search and seizure of a privately-owned computer or other privately owned communications device, or the contents thereof, that is in the system user's home.

Further, when he first started at the DoS in June 2008, Mr. Kim signed an "Internet Briefing Acknowledgement" and "Security Briefing for OpenNet+ Account" forms, both of which stated that he understood that his use of Government provided Internet and of his OpenNet+ account "may be monitored at any time." He also signed a "Waiver Statement Form," wherein he acknowledged that he understood that

- he did "not have a reasonable expectation of privacy concerning the data on [his] computer;"
- "All data contained on [his] computer may be monitored, intercepted, recorded, read, copied, or captured in any manner by authorized personnel. For example supervisors, system personnel or security personnel may give law enforcement officials any potential evidence of crime, fraud, or employee misconduct found on [his] computer."
- "Law enforcement may be authorized to access and collect evidence from [his] computer."
- "Authorized personnel will be routinely monitoring [his] computer for authorized purposes."
- "Consequently, any use of [his] computer by any user, authorized or unauthorized, constitutes DIRECT CONSENT to monitoring of [his] computer."

Similarly, while DoS policy permits limited personal use of the Internet and personal e-mail through an Internet connection, that policy also states:

Employees have no expectation of privacy while using any U.S. Government-provided access to

e-mail account to an e-mail account entitled [REDACTED]@yahoo.com. The e-mail from the Reporter forwarded another e-mail from other news reporters which included in its body a news article (not written by the Reporter) that would appear in the Washington Times (not the Reporter's news organization) the following day, July 12, 2009. This e-mail was found in the unallocated space located on Mr. Kim's DoS unclassified hard drive. I have been informed that when a computer file is deleted, the deleted file is flagged by the operating system as no longer needed, but remains on the hard disk drive in unallocated space unless the data is later overwritten.

32. Electronic evidence retrieved from Mr. Kim's DoS unclassified workstation also revealed that on September 24, 2009, following his interview with the FBI, Mr. Kim's user profile logged into the [REDACTED]@yahoo.com account through an DoS Internet connection accessed through his DoS unclassified workstation. DoS security badge access records suggest that Mr. Kim was in his VCI office suite where his DoS unclassified workstation was located when the [REDACTED]@yahoo.com account was accessed on September 24, 2009. While accessing that account on his DoS computer, Mr. Kim's user profile observed e-mails in that account from an e-mail account entitled [REDACTED]@gmail.com (which is the subject matter of the Government's request for a warrant here). Mr. Kim's profile also observed e-mails between the Reporter's work e-mail and [REDACTED]@yahoo.com, the e-mail account

the Internet. The Department considers electronic mail messages on U.S. Government computers, using the Internet or other networks, to be government materials and it may have access to those messages whenever it has a legitimate purpose for doing so. Such messages are subject to regulations and laws covering government records, and may be subject to Freedom of Information Act (FOIA) request or legal discovery orders."

5 FAM 723 (4).

identified by Mr. Kim as his own during his September 24, 2009 interview with the FBI, but which, one day later, he told the FBI was “full” and that he was “going to get rid of it.”

33. During the Internet session described above on September 24, 2009, Mr. Kim attempted to clear his “Temporary Internet Files.” I have been informed that deletion of Temporary Internet Files created by a web browser software application moves the cached content of internet sites visited to unallocated space, which, again, is space on the hard drive flagged by the operating system as being available for overwriting.

34. On November 9, 2009, search warrants were executed on both the [REDACTED]@yahoo.com and [REDACTED]@yahoo.com e-mail accounts. Those searches revealed multiple e-mails between Mr. Kim and the Reporter dating between May 11, 2009 and August 15, 2009. Review of those e-mails demonstrates that [REDACTED]@yahoo.com and [REDACTED]@yahoo.com are e-mail accounts used by Mr. Kim and [REDACTED]@gmail.com is an account used by the Reporter⁹ to receive e-mails from Mr. Kim and perhaps other sources. Further, in their e-mail communication, Mr. Kim and the Reporter appear to have employed aliases (i.e., Mr. Kim is “Leo” and the Reporter is “Alex”). The content of the e-mail communications also demonstrate that Mr. Kim was a source for the Reporter concerning the foreign country that was the subject matter of the June 2009 article (the “Foreign Country”) and that the Reporter solicited the disclosure of intelligence information from Mr. Kim concerning that country. A chronological listing and description of the most

⁹ “[REDACTED]” is not the name of the Reporter. Rather, this e-mail account was apparently named after a former Deputy Assistant to President Richard Nixon who is best known as the individual responsible for the secret taping system installed in the Nixon White House, and who exposed the existence of that taping system when he testified before Congress during the Watergate hearings.

pertinent e-mails is as follows:

- (a). A May 11, 2009 e-mail from [REDACTED]@yahoo.com to [REDACTED]@gmail.com reads:

I am back from my trip. Here is my personal information.

Please send me your personal cell number. I believe you have mine. It was great meeting you.

Thanks,

Stephen

(Mr. Kim attached to this e-mail his resume and a biographical description, both of which noted his access to classified information and his expertise concerning the Foreign Country).

- (b). A May 20, 2009 e-mail from [REDACTED]@gmail.com to [REDACTED]@yahoo.com responding to the above May 11, 2009 e-mail outlines a clandestine communications plan between Mr. Kim and the Reporter. In the e-mail, the Reporter solicits Mr. Kim as a source of sensitive and/or internal government documents (*italicized below*). It reads:

Your credentials have never been doubted – but I am nonetheless grateful to have the benefit of a chronological listing of your postings and accomplishments. I only have one cell phone number, on my Blackberry, which I gave you 202-[phone number for the Reporter]. Unfortunately, when I am seated in my booth at the State Department, which is much of every day, it does not get reception. thus [sic] I instruct individuals who wish to contact me simply to send me an e-mail to this address [REDACTED]@gmail.com]. *One asterisk means to contact them, or that previously suggested plans for communication are to proceed as agreed; two asterisks means the opposite.* With all this established, and presuming you have read/seen enough about me to know that I am trustworthy . . . let's get about our work! What do you want to accomplish together? As I told you when we met, I can always go on television and say: "*Sources tell [name of the Reporter's national news organization]*" But I am in a much better position to advance the interests of all concerned if I can say: "*[Name of the Reporter's national news organization] has obtained . . .*"

Warmest regards, [first name of Reporter].

[Emphasis added]

- (c). Another May 20, 2009 e-mail from [REDACTED]@gmail.com to [REDACTED]@yahoo.com, the body of which states:

Please forgive my delay in replying to you. I was on vacation out of town
....

Yours faithfully, [first name of Reporter]

- (d). A May 22, 2009 e-mail from [REDACTED]@gmail.com to [REDACTED]@yahoo.com in which the Reporter explicitly seeks from Mr. Kim the disclosure of intelligence information about the Foreign Country. It reads:

Thanks Leo. What I am interested in, as you might expect, is breaking news ahead of my competitors. I want to report authoritatively, and ahead of my competitors, on new initiatives or shifts in U.S. policy, events on the ground in [the Foreign Country], *what intelligence is picking up*, etc. As possible examples: I'd love to report that the IC¹⁰ *sees activity inside* [the Foreign Country] suggesting [description of national defense information that is the subject of the intelligence disclosed in the June 2009 article]. I'd love to report on what the hell [a named U.S. diplomat with responsibilities for the Foreign Country] is doing, maybe on the *basis of internal memos* detailing how the U.S. plans to [take a certain action related to the Foreign Country] (if that is really our goal). I'd love to see some *internal State Department analyses* about the state of [a particular program within the Foreign Country that was the subject matter of the June 2009 article], about [the leader of the Foreign Country]. . . . In short: Let's break some news, and expose muddle-headed policy when we see it – or force the administration's hand to go in the right direction, if possible. The only way to do this is to EXPOSE the policy, or *what the [Foreign Country] is up to*, and the only way to do that authoritatively is *with EVIDENCE*.

Yours faithfully, Alex.

[Emphasis added]

- (e). Mr. Kim forwarded an e-mail containing the above May 22, 2009 [REDACTED]@gmail.com e-mail to his [REDACTED]@yahoo.com at 10:57

¹⁰ "IC" is a common acronym denoting "Intelligence Community."

a.m. on the date of the June 2009 article. At the time of this e-mail, DoS badge records indicate that Mr. Kim and the Reporter were outside the DoS building, having left the building at approximately the same time. The content of the forwarded e-mail is blank, but the subject line is "Fw: Re: here."

- (f). In an e-mail dated in June 2009, following the publication of the June 2009 article, the Reporter forwarded from the Reporter's work e-mail account (which spells out the Reporter's name) to the [REDACTED]@yahoo.com account the following e-mail from another reporter associated with the Reporter's national news organization. It reads:

Hi [first name of Reporter] – wondering if you would like to check with your sources on something we are hearing but can't get totally nailed down over here.

It seems that the [U.S. Government is concerned about something related to the Foreign Country] and is watching it very closely . . . We can't get many more details than that right now – but our source said if we could find [a specific detail] elsewhere he would give us more. Though you might be able to squeeze out a few details and we could double team this one

Many thanks, dear friend,

[Name of second reporter associated with Reporter's national news organization]

The Reporter then forwarded the above e-mail asking for the Reporter to "squeeze out a few details" about the Foreign Country from the Reporter's "sources" to Mr. Kim at his [REDACTED]@yahoo.com account and included the following introductory note:

Leo: From the [Reporter's national news organization] Pentagon correspondent, I am at 202-[Reporter's office number at the Reporter's news organization] today.

Hugs and kisses, Alex¹¹

¹¹ One day after this e-mail was sent, toll records indicate that Mr. Kim placed a six-and-a-half minute phone call to the Reporter's office number at the Reporter's news organization (as requested in the above-referenced e-mail).

- (g). An e-mail dated in June 2009 from the Reporter's work e-mail to [REDACTED]@yahoo.com containing a subject referencing the Foreign Country. The content of the e-mail included only the Reporter's phone number next to an asterisk (*) which, according to the May 20, 2009 e-mail described above, was the Reporter's signal that Mr. Kim should call him.¹²
- (h). A July 11, 2009 e-mail from the Reporter's work e-mail to [REDACTED]@yahoo.com attaching, without comment, a news article *dated the following day* from another national news organization concerning the intelligence community.
- (i). A July 12, 2009 e-mail from the Reporter's work e-mail to [REDACTED]@yahoo.com attaching, without comment, a news article *dated the following day* from another national news organization concerning the Foreign Country.
- (j). An August 15, 2009 e-mail from the [REDACTED]@yahoo.com account to the Reporter's work e-mail account, which states:

Hope you are alright but I sense that they are not.

- (k). An August 15, 2009 e-mail from the Reporter's work e-mail responding to the above e-mail, and stating:

Leo,

You are most perceptive and I appreciate your inquiry. Call me at work on Monday [at the Reporter's work phone number] and I will tell you about my reassignment. In the meantime, enjoy your weekend!

Alex

(The electronic signature to this e-mail following the word "Alex" identifies the Reporter by the Reporter's full name, phone number, e-mail address, and media organization).

- 35. The FBI conducted a second non-custodial interview of Mr. Kim on March 29,

¹² On the date of this e-mail, Mr. Kim was traveling outside of the United States. Mr. Kim's toll records do not indicate that Mr. Kim called the Reporter after this e-mail was sent. They do indicate, however, that three minutes after this e-mail was sent, a 53 second call was placed from a number associated with the Reporter's news organization to Mr. Kim's cell phone.

2010. During the interview Mr. Kim made a number of admissions, including:

- confirming that the Owner's information disclosed in the June 2009 article was national defense information and most of it, in Mr. Kim's mind, was properly classified at the TOP SECRET/SCI level;
- confirming that the same disclosures in the June 2009 article were, in Mr. Kim's mind, "egregious," "bad" and harmful to the national security in a number of respects which he described in detail;
- acknowledging that, while he could not recall the specifics of the Intelligence Report, he was "fairly certain" he had reviewed it and agreed that if electronic records indicated that he had accessed the Report then he did so;
- agreeing that the Owner's information disclosed in the June 2009 article appeared to be derived from the Intelligence Report with only one difference that he described as a "subtle nuance;"
- acknowledging that he had received extensive training on the handling of classified information, and had executed multiple classified information non-disclosure agreements with the Government;
- confirming that he understood the TS/SCI classification markings that were prominently displayed on the Intelligence Report;
- admitting that the Owner's information disclosed in the June 2009 article, to his knowledge, did not "match" information in the public domain, but advising that "bits and pieces" of the article were possibly derived from open source information;
- acknowledging that he understood the security banner on the classified computer database and that his actions were subject to monitoring;
- re-stating his false statement from his interview with the FBI on September 24, 2009, that he had no contact with the Reporter after they first met in March 2009;
- after being confronted with the evidence of his extensive contacts with the Reporter in the months after they first met, (i) first stating that his calls with the Reporter had been facilitated by an unidentified "friend" and that he did not inform the FBI of his telephone contacts with the Reporter because he did not consider them "direct contacts;" but then later (ii) openly admitting during the interview that he had "lied" to the FBI about the extent of his relationship with the Reporter because he was "scared" that the FBI might investigate him for the leak;

- while denying that he had met face-to-face with the Reporter on the date of the June 2009 article, admitting that he had met with the Reporter outside of the DoS building at other times including once following the FBI's September 24, 2009 interview;
- admitting that the emails seized during the FBI's investigation were, in fact, emails between himself and the Reporter;
- admitting, after being asked the question a number of times, that "Leo Grace" was an alias used in the e-mails for himself and that "Alex" was an alias used by the Reporter, and
- while asserting that the [REDACTED]@yahoo.com account pre-dated his relationship with the Reporter, stating that it was the Reporter's idea to use covert e-mail communications as a means of compartmentalizing the information and a way for Mr. Kim to "feel comfortable talking with [the Reporter]."

36. According to the FBI agents who conducted the interview, during the interview, Mr. Kim never provided a coherent explanation for the evidence of his extensive contacts with the Reporter including on the date of the leak in question. At one point, he indicated that he was communicating with the Report hoping that the Reporter "could help put him in a think tank." Mr. Kim's reaction to the evidence was mostly stunned silence, although at one point he admitted that some of the evidence was "very disturbing." Nevertheless, Mr. Kim denied that he was a source for the Reporter or had knowingly provided the Reporter with classified documents or information. Mr. Kim claimed to have specifically informed the Reporter that the Reporter "won't get stuff out of me," to which the Reporter allegedly replied, "I don't want anything." Mr. Kim did admit, however, that he may have "inadvertently" confirmed information that he believed the Reporter had already received from other individuals. Mr. Kim made further

statements which could fairly be characterized as either a confession or a near confession¹³:

- “I did not purposely discuss the [Intelligence Report], but might have discussed [some of the topics discussed in the Report].”
- “Maybe I inadvertently confirmed something . . . too stubborn to not . . . [I] just don’t know . . . someone values my views, listens up, . . . maybe I felt flattered. [The Reporter] is a very affable, very convincing, persistent person. [The Reporter] would tell me I was brilliant and it is possible I succumbed to flattery without knowing it. Maybe it was my vanity. [The Reporter] considers me an expert and would tell me . . . could use my insight. . . . The IC is a big macho game but I would never say I’m read in to this and you are not. I would never pass [the Reporter] classified.”
- “[The Reporter] exploited my vanity.”
- “[M]y personal and professional training told me not to meet people like [the Reporter]. I felt like while on the phone I was only confirming what he already knew. I was exploited like a rag doll. [The Reporter] asked me a lot of questions and got me to talk to him and have phone conversations with him. [The Reporter] asked me a lot, not just specific countries. [The Reporter] asked me how nuclear weapons worked.”
- “It’s apparent I did it. I didn’t say ‘did you see this?’ I think I did it. I can’t deny it. I didn’t give [the Reporter] the [specific intelligence information in the article]. I didn’t provide him with the stuff.”
- “I don’t think I confirmed . . . maybe I inadvertently confirmed in the context of other conversations [with the Reporter]. It wasn’t far-fetched that the information was out there. I would not talk over an open line about intelligence. I did not leak classified.”
- Finally, Mr. Kim opined that “someone either gave [the Reporter] the [the Intelligence Report] or it was read to [the Reporter] over the telephone.”

37. During his interview, Mr. Kim also consented to a physical search of his condominium in McLean, Virginia. No hard-copy classified documents or other hard-copy materials directly related to the leak at issue were found during the search of Mr. Kim’s

¹³ The FBI interview was not audio or video taped. What follows are excerpts from an FBI report memorializing the interview.

condominium. During the search the FBI recovered three computers that are presently being analyzed. Thus far, no information relevant to this investigation has been identified on those computers.

38. The text of the June 2009 article reflects the Reporter's knowledge and understanding that the information the Reporter had received was intelligence information the disclosure of which could be harmful to the United States.

39. I conclude from the foregoing that there is probable cause to believe that:

- (a). From the beginning of their relationship, the Reporter asked, solicited and encouraged Mr. Kim to disclose sensitive United States internal documents and intelligence information about the Foreign County. Indeed, in the May 20, 2009 e-mail, the Reporter solicits from Mr. Kim some of the national defense intelligence information that was later the subject matter of the June 2009 article;
- (b). The Reporter did so by employing flattery and playing to Mr. Kim's vanity and ego;
- (c). Much like an intelligence officer would run an clandestine intelligence source, the Reporter instructed Mr. Kim on a covert communications plan that involved the e-mail of either one or two asterisks to what appears to be a e-mail account set up by the Reporter, [REDACTED]@gmail.com, to facilitate communication with Mr. Kim and perhaps other sources of information;
- (d). To conceal further their communications, the Reporter and Mr. Kim employed aliases in their e-mail communication to each other (i.e., Mr. Kim is "Leo" and the Reporter is "Alex");
- (e). The Reporter was in repeated telephone contact with Mr. Kim prior to, and on the day of, the leak of the classified information in question;
- (f). On the day of the leak, Mr. Kim was on the telephone with the Reporter at or around the same time that Mr. Kim was viewing the Intelligence Report containing TOP SECRET/SCI national defense information about the Foreign Country;
- (g). The text of the June 2009 article reflects the Reporter's knowledge and understanding that the information the Reporter had received was intelligence

information the disclosure of which could be harmful to the United States;

- (h). Nevertheless, the Reporter published an article on the Internet containing the TOP SECRET/SCI national defense information about the Foreign Country that was in the Intelligence Report;
- (i). Thereafter, it appears the Reporter (i) returned the favor by providing Mr. Kim with news articles *in advance of their publication* concerning intelligence matters and the Foreign Country and (ii) continued to contact Mr. Kim as a source when the Reporter's colleagues needed sensitive government information about the Foreign Country.

40. Based on the foregoing, there is probable cause to believe that the Reporter has committed a violation of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information), at the very least, either as an aider, abettor and/or co-conspirator of Mr. Kim.

III. ITEMS TO BE SEIZED

41. Further, based on the foregoing, there is probable cause to believe that evidence material to this investigation will be found in the [REDACTED]@gmail.com account. While the searches of Mr. Kim's e-mail accounts have revealed a number of e-mails between Mr. Kim and the Reporter, certain of those e-mails indicate that there are additional e-mail communications that have not been recovered by the FBI and that, if they still exist, would likely be found in the [REDACTED]@gmail.com account. Specifically, the searches of Mr. Kim's [REDACTED]@yahoo.com e-mail account did not reveal his responses to the May 20, 2009 or May 22, 2009 e-mails from the Reporter soliciting sensitive, internal and/or intelligence information about the Foreign Country. The May 22, 2009 e-mail from the Reporter, for example, begins "Thanks Leo. What I am interested in, as you might expect, is breaking news ahead of my competitors." Thus, the May 22nd e-mail is a response from the Reporter to an earlier e-mail from Mr. Kim apparently inquiring as to what kind of information the Reporter

was interested in receiving. Further, the subject line of the e-mail is "Re: here," indicating that there was a prior e-mail from Mr. Kim to the Reporter with the subject line "here." That e-mail – sent from Mr. Kim to the Reporter just following the Reporter's May 20, 2009 solicitation of information from Mr. Kim – was not found in the searches of Mr. Kim's e-mail accounts. It is reasonable to believe that this and other e-mails *sent from* Mr. Kim to the Reporter would exist in the "in-box" of the [REDACTED]@gmail.com account. Mr. Kim's missing responses to the Reporter's e-mails would materially assist the FBI's investigation as they could be expected to establish further the fact of the disclosures, their content, and Mr. Kim's and the Reporter's intent in making them, and could be expected to constitute direct evidence of their guilt or innocence.

42. The June 2009 article was published on June 11, 2009. The Owner's information published in that article was first disseminated to representatives of the United States on June 10, 2009.

43. Further, it would materially assist the FBI's investigation to review all e-mails in the Reporter's [REDACTED]@gmail.com account on these two days to potentially establish by direct evidence the fact of the disclosures. Further, because we know that Mr. Kim was in contact with the Reporter through this account, it is reasonable to believe that any other sources the Reporter may have had with regard to the Foreign Country, if any, would similarly use the [REDACTED]@gmail.com account to communicate with the Reporter, particularly given the statement in the May 20, 2009 e-mail that the Reporter "instructs individuals who want to reach" the Reporter to send an e-mail to that account.

44. Accordingly, the FBI submits that Google should be ordered to produce in

response to this warrant:

- (i) all communications, on whatever date, between [REDACTED]@gmail.com and Mr. Kim's known e-mail accounts, i.e., [REDACTED]@yahoo.com, [REDACTED]@yahoo.com, and [REDACTED]@gmail.com;¹⁴ and
- (ii) all communications "to" or "from" the [REDACTED]@gmail.com on June 10th and 11th, 2009.

45. While it is not required for a warrant to issue under section 2000aa, the FBI has exhausted all reasonable non-media alternatives for collecting the evidence it seeks. We seek e-mails between the Reporter and Mr. Kim that we have probable cause to believe existed. To gather that evidence, we have the option of searching either the Reporter's or Mr. Kim's e-mail accounts. Our searched of Mr. Kim's e-mail accounts have not yielded all the e-mails between him and the Reporter that our evidence to date demonstrates exist. Other than asking the Reporter for a voluntary production of the e-mails from the [REDACTED]@gmail.com account, there is no other way to get the evidence we rightfully seek. Because of the Reporter's own potential criminal liability in this matter, we believe that requesting the voluntary production of the materials from Reporter would be futile and would pose a substantial threat to the integrity of the investigation and of the evidence we seek to obtain by the warrant.

46. Based on the above, there is probable cause to believe that the Reporter (along with Mr. Kim) has committed a violation of 18 U.S.C. § 793(d) either as Mr. Kim's co-conspirator and/or aider and abettor, and that evidence of that crime is likely contained within the [REDACTED]@gmail.com account. Accordingly, the FBI's request to search the contents of

¹⁴ A Google representative has indicated that, if ordered by a court as part of a search warrant, Google can produce e-mail communications between certain e-mail accounts.

that account falls squarely within section 2000aa(a)'s exception permitting searches of media-related work product materials, even when possessed by a national news reporter because there is "probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate." 42 U.S.C. § 2000aa(a).

47. On October 2, 2009, the FBI submitted a preservation letter to Google, pursuant to 18 U.S.C. § 2703(f), requesting that the contents of [REDACTED]@gmail.com be preserved. On January 15, 2010, a second preservation letter for the account was sent to Google. This second preservation letter was 15 days over the 90-day limit for preservation prescribed by 18 U.S.C. § 2703(f). Thus, there remains the possibility that relevant content in the account has been deleted.¹⁵ Nevertheless, we consider that possibility remote because, to the FBI's knowledge, in January 2010, neither Mr. Kim nor the Reporter knew that Mr. Kim was a target of this investigation nor that the existence of the [REDACTED]@gmail.com account was known to the FBI. On April 9, 2010, another 90-day extension of the preservation order was permitted by Google, Inc. for the account.

IV. COMPUTERS, THE INTERNET, AND E-MAIL

48. I have received training from the FBI related to computer systems and the use of computers during criminal investigations. Based on my education, training and experience, and information provided to me by other law enforcement agents, I know the following:

- (a). The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. The term "computer", as used herein, is defined in 18 U.S.C. § 1030(e)(1) and includes an electronic, magnetic, optical, electrochemical, or

¹⁵ On January 21, 2010, Google refused to confirm to an FBI agent whether there is any content in the account without service of formal process.

other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. A computer user accesses the Internet through a computer network or an Internet Service Provider (ISP).

- (b). E-mail, or electronic mail, is a popular method of sending messages and files between computer users. When a computer user sends an e-mail, it is created on the sender's computer, transmitted to the mail server of the sender's e-mail service providers, then transmitted to the mail server of the recipient's e-mail service provider, and eventually transmitted to the recipient's computer. A server is a computer attached to a dedicated network that serves many users. Copies of e-mails are usually maintained on the recipient's e-mail server, and in some cases are maintained on the sender's e-mail server.

49. Based on my training and experience, and information provided to me by other law enforcement agents, I know the following: First, searches of e-mail accounts usually provide information that helps identify the user(s) of the e-mail accounts. Second, individuals who use e-mail in connection with criminal activity, or activity of questionable legality, often set up an e-mail account to be used solely for that purpose. This is often part of an effort to maintain anonymity and to separate personal communication from communication and information that is related to the criminal activity. Third, when the criminal violation involves a conspiracy, a search of an e-mail account often allows the identification of any co-conspirators.

V. BACKGROUND REGARDING GOOGLE

50. Based on my training and experience, I have learned the following about Google:
- (a). Google is an internet services company that, among other things, provides e-mail services (known as gmail). Subscribers obtain an account by registering on the Internet with Google. Google requests subscribers to provide basic information, such as name, gender, zip code and other personal/biographical information. However, Google does not verify the information provided.
 - (b). Google is located at 1600 Amphitheatre Parkway, Mountain View, California. Google maintains electronic records pertaining to the subscribers of its e-mail

services. These records include account access information, e-mail transaction information, and account application information.

- (c). Subscribers to Google may access their Google accounts using the Internet.
- (d). E-mail messages and files sent to a gmail account are stored in the account's "inbox" as long as they are not identified as "SPAM," the account has not exceeded the maximum storage limit, and the account has not been set to forward messages or download to an e-mail client with the option "delete gmail's copy." If the message/file is not deleted by the subscriber, the account is below the maximum storage limit, and the account has not been inactivated, then the message/file will remain on the server indefinitely. E-mail messages and files sent from a gmail account will remain on the server indefinitely unless they are deleted by the subscriber.
- (e). Google provides POP3 access for gmail accounts. POP3 is a protocol by which e-mail client software such as Microsoft Outlook or Netscape Mail can access the servers of an e-mail service provider and download the received messages to a local computer. If POP3 access is enabled, the account user can select to keep a copy of the downloaded messages on the server or to have the messages deleted from the server. The default setting for gmail accounts is to keep a copy of the messages on the server when POP3 access is enabled. Gmail subscribers can also access their accounts through an e-mail client such as Microsoft Outlook by using the IMAP protocol. When gmail subscribers access their accounts through IMAP, a copy of the received messages remains on the server unless explicitly deleted.
- (f). A Google subscriber can store files, including e-mails, text files, and image files, in the subscriber's account on the servers maintained and/or owned by Google.
- (g). E-mails and other files stored by a Google subscriber in a Google account are not necessarily also located on the computer used by the subscriber to access the Google account. The subscriber may store e-mails and other files in their Google account server exclusively. A search of the files in the subscriber's computer will not necessarily uncover the files that the subscriber has stored on the Google server. In addition, communications sent to the Google subscriber by another, but not yet retrieved by the subscriber, will be located on the Google server in the subscriber's account, but not on the computer used by the subscriber.
- (h). Computers located at Google contain information and other stored electronic communications belonging to unrelated third parties. As a federal agent, I am trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of Google are not. I also know that the manner in which the data is preserved and analyzed may be critical to the

successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital evidence. Google employees are not. It would be inappropriate and impractical, however, for federal agents to search the vast computer network of Google for the relevant accounts and then to analyze the contents of those accounts on the premises of Google. The impact on Google's business would be severe.

VI. STORED WIRE AND ELECTRONIC COMMUNICATIONS

51. 18 U.S.C. §§ 2701–2711 is called the “Electronic Communications Privacy Act.”

(a). 18 U.S.C. § 2703(a) provides, in part:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b). 18 U.S.C. § 2703(b) provides, in part:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –

(A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service –

(A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission

from), a subscriber or customer of such remote computing service;
and

(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

- (c). The Government may also obtain records and other information pertaining to a subscriber or customer of an electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A). No notice to the subscriber or customer is required. 18 U.S.C. § 2703(c)(2).

- (d). 18 U.S.C. § 2711 provides, in part:

As used in this chapter – (1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and (2) the term “remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system.

- (e). 18 U.S.C. § 2510 provides, in part:

(8) “contents,” when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;...(14) “electronic communications system” means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; (15) “electronic...communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications;... (17) “electronic storage” means - (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

- (f). 18 U.S.C. § 2703(g) provides, in part:

Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

VII. REQUEST FOR NON-DISCLOSURE BY PROVIDER

52. Pursuant to 18 U.S.C. § 2705(b), this Court can enter an order commanding the PROVIDER not to notify any other person, including the subscriber of the SUBJECT ACCOUNT, of the existence of the warrant because there is reason to believe that notification of the existence of the warrant will result in: (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering of evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardize the investigation. The involvement of the SUBJECT ACCOUNT as set forth above is not public and I know, based on my training and experience, that subjects of criminal investigations will often destroy digital evidence if the subject learns of an investigation. Additionally, if the PROVIDER or other persons notify anyone that a warrant has been issued on the SUBJECT ACCOUNT, the targets of this investigation and other persons may further mask their identity and activity, flee, or otherwise obstruct this investigation. Accordingly, I request that this Court enter an order commanding the PROVIDER not to notify any other person, including the subscriber of the SUBJECT ACCOUNT, of the existence of the warrant.

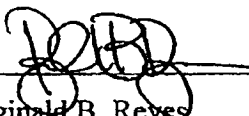
VIII. REQUEST FOR SEALING

53. Because this investigation is continuing and disclosure of some of the details of this affidavit may compromise subsequent investigative measures to be taken in this case, may

cause subjects to flee, may cause individuals to destroy evidence and/or may otherwise jeopardize this investigation, I respectfully request that this affidavit, and associated materials seeking this search warrant, be sealed until further order of this Court. Finally, I specifically request that the sealing order not prohibit information obtained from this warrant from being shared with other law enforcement and intelligence agencies.

IX. CONCLUSION

54. Based on the foregoing, there is probable cause to believe that the Reporter has committed or is committing a violation of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information), as an aider, abettor and/or co-conspirator, and that on the computer systems owned, maintained, and/or operated by Google, Inc., there exists in, and related to, the SUBJECT ACCOUNT, evidence, fruits, and instrumentalities of that violation of section § 793. By this affidavit and application, I request that the Court issue a search warrant directed to Google, Inc., allowing agents to seize the content of the SUBJECT ACCOUNT and other related information stored on the Google servers as further described and delimited in Attachment A hereto.


 Reginald B. Reyes
 Special Agent
 Federal Bureau of Investigation

Sworn to and subscribed before me
 on this MAY 28 2010 day of May


 United States Judge

ALAN KAY
U.S. MAGISTRATE JUDGE

EXHIBIT S

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT)
FOR E-MAIL ACCOUNT)
[REDACTED]@GMAIL.COM)
MAINTAINED ON COMPUTER SERVERS)
OPERATED BY GOOGLE, INC.,)
HEADQUARTERED AT)
1600 AMPHITHEATRE PARKWAY,)
MOUNTAIN VIEW, CA)

Mag. No.: 10-291-M-01

UNDER SEAL

FILED

NOV 6 2011

Clerk, U.S. District Court
Courts for the District of Columbia

ORDER

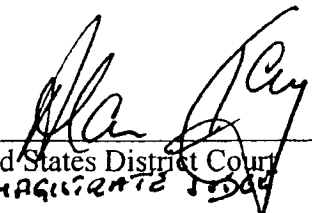
After reviewing the Government's Motion for Unsealing Search Warrant and Related Materials, it is hereby

ORDERED that the Government's motion is **GRANTED**; it is

FURTHER ORDERED that, to protect the privacy of the individuals involved, the attached redacted versions of the application for search warrant in this matter, the affidavit in support of the application for search warrant, the search and seizure warrant, and the Attachment A thereto, be **UNSEALED** and placed on the public record; and it is

FURTHER ORDERED that the Government may produce unredacted versions of this same material to the defense in United States v. Stephen Jin-Woo Kim, Cr. No. 10-225 (CKK), pursuant to the Rule 16 Protective Order in that matter.

SO ORDERED this 7th day of November 2011.


United States District Court
U.S. MAGISTRATE JUDGE

(N)